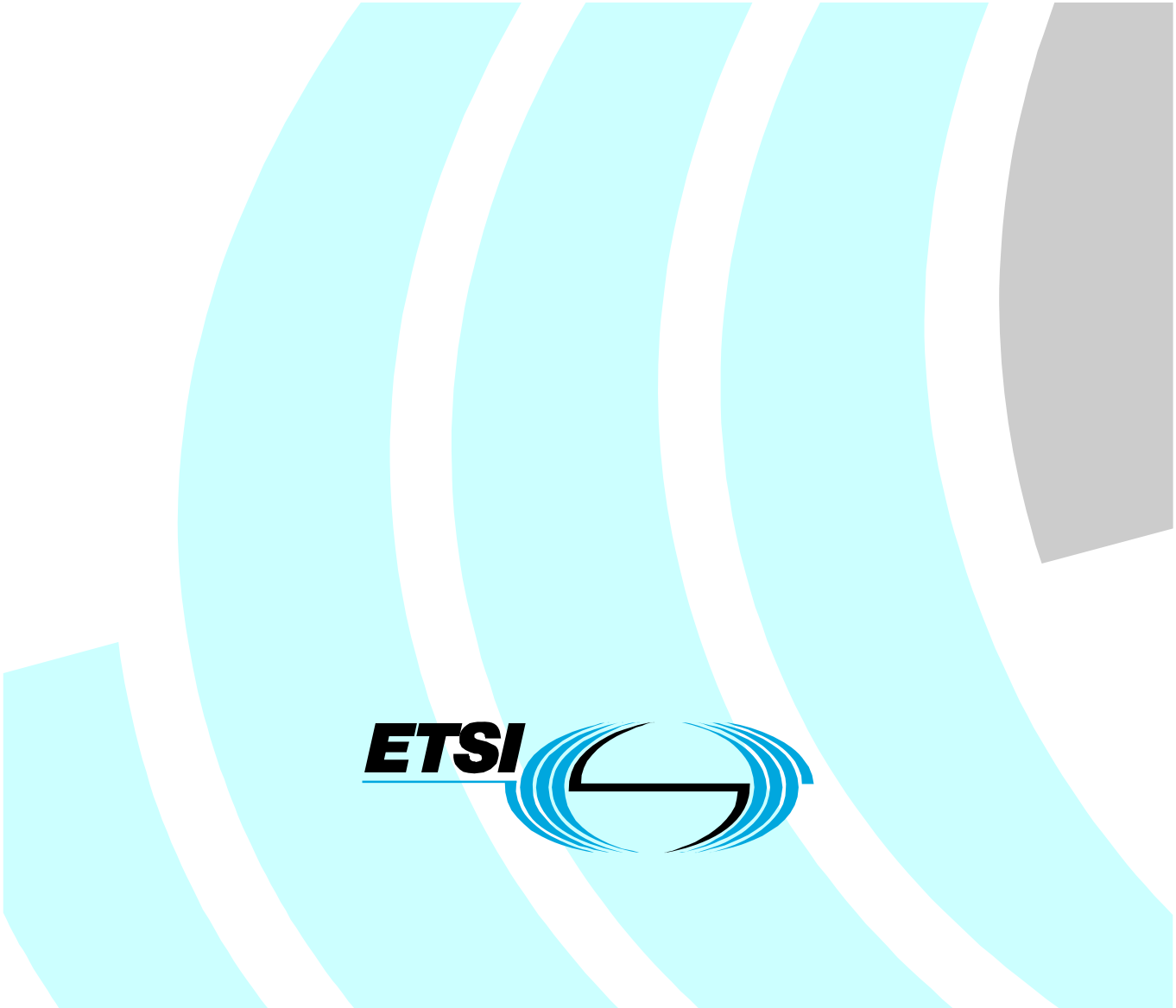
ETSI TR 102 745 V1.1.1 (2009-10)

Technical Report

Reconfigurable Radio Systems (RRS); User Requirements for Public Safety



Reference
DTR/RRS-04006

Keywords
radio, user

ETSI

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

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

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

Contents

Intellectual Property Rights

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

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

Foreword

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

Introduction

The present document provides an overview of the User Requirements for the application of RRS in the Public Safety and Defense domain.

1 Scope

The present document describes needs, applications and drivers for the application of RRS to the public safety.

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] ETSI TS 102 181: "Emergency Communications (EMTEL); Requirements for communication between authorities/organizations during emergencies".

[i.2] SDR Forum: "Use Cases for Cognitive Applications in Public Safety Communications Systems - Volume 1: Review of the 7 July Bombing of the London Underground".

NOTE: Available at: http://www.sdrforum.org/pages/documentLibrary/documents/SDRF-07-P-0019-V1_0_0.pdf

[i.3] ETSI TS 170 001 (V3.3.1): "Project MESA; Service Specification Group - Services and Applications; Statement of Requirements (SoR)".

[i.4] SAFECOM, US communications program of the Department of Homeland Security. "Public safety Statements of Requirements for communications and interoperability v I and II".

[i.5] ETSI TR 102 182: "Emergency Communications (EMTEL); Requirements for communications from authorities/organisations to the citizens during emergencies".

[i.6] ETSI TR 102 180: "Basis of requirements for communication of individuals with authorities/organizations in case of distress (Emergency call handling)".

[i.7] ETSI TR 102 410: "Emergency Communications (EMTEL); Basis of requirements for communications between individuals and between individuals and authorities whilst emergencies are in progress".

[i.8] ETSI TR 102 021: "Terrestrial Trunked Radio (TETRA); User Requirement Specification TETRA Release 2".

[i.9] ITU-R Recommendation BO.1774: "Use of satellite and terrestrial broadcast infrastructures for public warning, disaster mitigation and relief".

[i.10] ITU-R Recommendation S.1001: "Use of systems in the fixed-satellite service in the event of natural disasters and similar emergencies for warning and relief operations".

[i.11] ETSI TR 170 003: "Project MESA; Service Specification Group - Services and Applications; Basic requirements".

[i.12] ETSI TR 102 682: "Reconfigurable Radio Systems (RRS); Functional Architecture (FA) for the Management and Control of Reconfigurable Radio Systems".

[i.13] ETSI TS 102 734: "Electronic Signatures and Infrastructures; Profiles of CMS Advanced Electronic Signatures based on TS 101 733 (CAdES)".

[i.14] ETSI TR 102 733: "Reconfigurable Radio Systems (RRS); System Aspects for Public Safety".

[i.15] ITU-R Report M. 2033: "Radiocommunication objectives and requirements for public protection and disaster relief".

[i.16] ECC REPORT 102. Public protection and disaster relief spectrum requirements, Helsinki, January 2007.

[i.17] SeBoCom Pre-Study - A preliminary study on Secure Border Communications. European Commission Technical Report - EUR 23536 EN.

[i.18] World Radiocommunication Conference in 2003, resolution 646: "Public protection and disaster relief".

[i.19] SDR Forum: "Use Cases for Cognitive Applications in Public Safety Communications Systems" - Volume 1: Review of the 7 July Bombing of the London Underground.

[i.20] SDR Forum: "Utilization of Software Defined Radio Technology for the 700 MHz Public/Private Partnership".

[i.21] SDR Forum: "High Level SDR Security Requirements".

[i.22] CHORIST Project: "Report on user requirements and initial support cases".

[i.23] CHORIST Project: "Report on user needs and interoperability requirements".

[i.24] OASIS Project: "Definition of the OASIS Tactical Situation Object (D-TA2_06).

[i.25] OASIS Project: "OASIS User Requirements synthesis (D-TA2_01).

[i.26] WIDENS Project: "Users Requirements and First System Architecture Design (D2.1)".

[i.27] WIN Project: "User Requirements Specifications".

[i.28] WISECOM Project: "Survey of Use Cases. Deliverable 1.1-1".

[i.29] WISECOM Project: "User and System Requirements for Emergency Telecommunication Services. Deliverable 1.2-1".

[i.30] TETRA RELEASE 2: "User Requirement Specifications. URS 101-021-1 General Overview User Requirement Specification (URS) and URS 101-021-2 High Speed Data (HSD)".

3 Definitions and abbreviations

3.1 Definitions

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

cognitive radio: 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 (CR): radio system, which has the following capabilities:

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

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

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

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

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

public safety organization: organization 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

3.2 Abbreviations

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

AAF	Adaptive Ad-hoc Freeband
BAPCO	British Association of Public Safety Communications Officers
BER	Bit Error Rate
CEPT	Conférence des Administrations Européenes des Postes et Télécommunications
COI	Community of Interest
ECC	Electronic Communication Committee of the CEPT
EVM	Error Vector Magnitude
FA	Functional Architecture
GMDSS	Global Maritime Distress Safety System
PMR	Private Mobile Radio, Professional Mobile Radio

PPDR	Public Protection and Disaster Relief
PSRG	Public Safety Radiocommunications Group
RAT	Radio Access Technology
RRS	Reconfigurable Radio Systems
SDR	Software Defined Radio
TETRA	TErrestrial Trunked RAdio
USR	User Requirement Specification

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.

NOTE: As described in clause 1, the scope of the present document is to define the User Requirements for the application of RRS in the Public Safety and Defense 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.

Furthermore existing Public Safety standards already satisfy many Public Safety requirements, which are automatically supported by the RRS through the related waveforms.

4.1 Organizations

4.1.1 BAPCO (British Association of Public Safety Communication Officers)

BAPCO is an independent, user led, professional members Association to promote, influence and advance the development and use of communications and information management systems for the safety and security of the public.

One of the objectives of BAPCO is to promote the development of efficient and effective communications and supporting information technologies to provide value for money and effective systems to enhance delivery of public safety and civil contingency services for the benefit of the public and for the benefit of individual public safety and civil contingency services and personnel.

4.1.2 ECC

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

ECC is responsible for:

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. Public protection and disaster relief spectrum requirements, Helsinki, January 2007 [i.16], clause 7 presents the operational requirements for public safety radio communication.

4.1.3 ETSI EMTEL

ETSI Special Committee EMTEL is responsible for identifying the operational and technical requirements of those involved in the provision of emergency communications, for conveying these requirements to other ETSI committees and for liaison with other organizations involved in this field.

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 requirements definition:

- Requirements for communication of citizens with authorities/organizations in case of distress (emergency call handling), see TR 102 180 [i.6].
- Emergency Communications (EMTEL); Requirements for communication between authorities/organizations during emergencies, see TS 102 181 [i.1].
- Emergency Communications (EMTEL); Requirements for communications from authorities/organizations to individuals, groups or the general public during emergencies, see TR 102 182 [i.5].
- Communications between individuals and between individuals and authorities during emergencies, see TR 102 410 [i.7].

4.1.4 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 & Gas

The following documents are relevant for requirements definition:

- User Requirement Specification TETRA Release 2. See TR 102 021 [i.8].
- Technical Reports from TETRA Working Group 1, which is responsible for producing the User Requirement Specification (URS) for development and enhancement of TETRA.

4.1.5 FRONTEX

Frontex, the EU agency based in Warsaw, was created as a specialized and independent body tasked to coordinate the operational cooperation between Member States in the field of border security.

A number of joint operations (Sea, Land and Air) have been organized by FRONTEX at European level, which can provide useful input for the requirements definition.

FRONTEX has also organized a number of workshops, where representatives from Public Safety organizations present and discuss operational needs and requirements. Recently the SEBOCOM workshop was organized with JRC - EC for "Secure Border Communications".

The output of the workshop can also be relevant for requirements definition:

- SeBoCom Pre-Study - A preliminary study on Secure Border Communications. European Commission Technical Report - EUR 23536 EN. [i.17].

4.1.6 ITU

International Telecommunication Union (ITU) has investigated the use of communications for public protection and disaster relief (PPDR).

An important agreement concerning public protection and disaster relief was reached at the World Radiocommunication Conference in 2003 (WRC-03) in Resolution 646 [i.18]. It supports the deployment of new technologies for enhanced applications involving higher data rates, real-time full motion video and multimedia services that should facilitate the work of PPDR agencies around the world.

The following documents are relevant for requirements definition:

- ITU-R Report M. 2033 [i.15]. Radiocommunication Objectives and Requirements for Public Protection and Disaster Relief (PPDR). The document defines objectives and needs for the implementation of future PPDR solutions. The document focuses on operational needs around 2010.

- ITU-R Recommendation BO.1774 [i.9]
  "Use of satellite and terrestrial broadcast infrastructures for public warning, disaster mitigation and relief".

- ITU-R Recommendation S.1001 [i.10]
  "Use of systems in the fixed-satellite service in the event of natural disasters and similar emergencies for warning and relief operations".

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.

NATO has produced a number of documents relevant for requirements definition especially in case of joint interoperability between Public Safety and Defense.

4.1.8 PSRG (Public Safety Radio communication Group)

The objectives from the PSRG is to create a co-operative forum to exchange information to facilitate the introduction, deployment and benefits realization of digital mobile radio services for (national) Public Safety bodies, covering issues like user aspects, technical (e.g. frequency aspects), procurement, project management, operational, education/training benefits and knowledge regarding the different projects. The members should have a role in the project from their country.

4.1.9 PSCE (Public Safety Communication Europe)

PSCE is also called the NARTUS project. It is focused on establishing and facilitating a Forum for regular exchange of ideas, information, experiences and best practices, and on seeking agreement among participating stakeholders.

Project NARTUS is completed on June 2009 and PSCE is continuing in self-sustaining mode.

The following documents are relevant for requirements definition:

- D1.3 "Test case and validation scenarios".

- D2.2 "Report on mapping of technologies on first operational scenarios".

- D3.13 "Market Studies Report".

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 requirements definition:

- Reference [i.4] "Public safety Statements of Requirements for communications and interoperability v I and II. Volume I explains the qualitative requirements and identifies the applications and services critical for public safety communications. Volume II describes the quantitative requirements and provides detailed quality of service methods of measurement for the applications and services identified in Volume I, along with network parameters to specify the minimum acceptable performance of public safety communications systems carrying these services" (from Safecom web site).

In the document Public safety Statements of Requirements for communications and interoperability v I and II, a number of scenarios are described.

From [i.4]:

- EMS: Routine Patient Services and Car Crash Scenario. A voice conference call is set up between the ambulance and the hospital, while the vehicle's geolocation as well as the vital measurements and treatments of the patient are recorded and transmitted wirelessly.

- A residential fire scenario: as in the first scenario, geolocation and vital measurements of multiple victims, first responders and vehicles is wirelessly transmitted; additionally, GIS information on building plans, fire hydrant locations, etc. is accessible.

- A traffic stop scenario: the situation message, the police vehicle's ID and geolocation are transmitted; the suspect car's license plate is read and sent to dispatch, where it is queried against several law enforcement databases, and the results are sent back to the police officer; a video stream of the action is available on demand to dispatch; the officer decides to request backup, the nearest vehicle is located by the backup system and the request is forwarded; when the suspect is arrested, information about the crime, the police officer, etc. is loaded onto the RFID embedded in the handcuffs; after the arrest, biometric data from the suspect is sent to dispatch, queried against databases, and the answers are sent back; the officer communicates with the tow truck company; evidence and other information is transmitted to the sheriff's office; the case report is sent electronically to the officer's supervisor.

- An explosion scenario: here the communications analysis is from the incident commander's point-of-view, while all the first-responder requirements described in the previous scenarios are still considered valid; the various (diverse) units that arrive on the scene form an ad-hoc overlay network and provide information about their location and status; GIS information is available on demand to the commanders; distributed sensors on the first-responders relay their readings to central command; a secondary perimeter is set up, and a reverse 911 call is sent to fixed and mobile users (civilian) inside the perimeter to evacuate or find shelter; at the same time, the Department of Transportation is notified to divert traffic from the area; critical infrastructure (gas, electricity) is shut down; the commander decides the explosion is not an accident, and directs field agents to treat it as a crime scene, while calling in detectives to investigate; the number of casualties is assessed too high for local hospitals, so coordination with other medical centres is necessary; at the end of the incident all-but-one of each type of team is released.

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 requirements definition:

- Use Cases for Cognitive Applications in Public Safety Communications Systems - Volume 1: Review of the 7 July Bombing of the London Underground [i.19].

NOTE: Some WG4 members did not consider this document useful for the WG4 activity.

- Utilization of Software Defined Radio Technology for the 700 MHz Public/Private Partnership [i.20]. Even if the document is focused on the US 700 MHz band, some considerations apply to this working group as well.

- High Level SDR Security Requirements [i.21]. This document is not directly related to User Requirements but it still provides useful input for requirements definition.

4.1.12 TETRA Association

(From TETRA Association web site): "The TETRA MoU (Memorandum of Understanding), now known as the TETRA Association, was established in December 1994 to create a forum which could act on behalf of all interested parties, representing users, manufacturers, application providers, integrators, operators, test houses and telecom agencies. Today the TETRA Association represents more than 150 organizations from all continents of the world.

The goal for the TETRA Association is to provide a forum for all those interested in TETRA to encourage adoption of the standard and support initiatives to obtain appropriate levels of spectrum such that growth in operational TETRA systems is not restricted by regulation". (From http://www.tetra-association.com/).

The following documents are relevant for requirements definition:

- TETRA RELEASE 2 User Requirement Specifications.
  Especially: 101-021-1 General Overview User Requirement Specification (URS). 101-021-2 High Speed Data (HSD) URS [i.30].

4.2 Projects

4.2.1 AAF Project (Adaptive Ad-hoc Freeband communication)

The AAF project investigated the use of Cognitive Radio in emergency situations and especially in relation to the deployment of ad-hoc networks to resolve emergency crisis and natural disasters.

As a research project, AAF investigate the benefits of Cognitive Radio, especially in relation to the problem of spectrum scarcity and lack of network resources, which is exasperated during an emergency crisis as network infrastructures may be degraded or panic conditions may increase the traffic overload. AAF identified trade-offs and solutions to support deployment of ad-hoc cognitive networks.

4.2.2 Project CHORIST

Project CHORIST (integrating communications for enhanced environmental risk management and citizens safety) is a 3-year project (June 2006 - May 2009), funded by the European Commission, which addresses Environmental Risk Management in relation to natural hazards and industrial accidents. More details on the project are described in http://www.chorist.eu.

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 requirements definition:

- Report on user requirements and initial support cases (SP1.D4) [i.22].

- Report on user needs and interoperability requirements (SP4.D1) [i.23].

Project CHORIST has put considerable effort in the analysis of existing requirements and their definition. As a consequence the deliverable mentioned above is particularly valuable to the present document even if they are not addressed specifically to RRS technologies.

Deliverable SP4.1 identifies user's services and three classes of user requirements: general requirements, technical management requirements and tactical management requirements. The user services are voice services, data services, security services and interoperability. Examples of general requirements are dynamic configuration, self-healing capabilities, RF efficiency and so on. Technical management requirements are traffic management configuration,

monitoring, fixed structure access and events generation and collecting. Operational requirements are scaling for traffic and coverage and restorability.

Some of these requirements are valid also for RRS-based communication network and they have been adopted in the present document.

CHORIST defined three operational scenarios to validate the requirements:

1) an hurricane scenario;

2) flooding with risk of landslides; and

3) an accident in a chemical industrial plant.

CHORIST identified the lack of broadband communication as a major issue in the current context of public safety communications. WiMAX technology and TETRA TEDS have been evaluated as possible solution to overcome this challenge.

4.2.3 ESSOR

The ESSOR study, planned to be a Cat B program under the auspices of the EDA, 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.

4.2.4 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 requirements definition:

- Service Specification Group Services and Applications;
  Statement of Requirements (TS 170 001 [i.3])

- Service Specification Group - Services and Applications;
  Basic requirements (TR 170 003 [i.11])

Project MESA had a major influence in the definition of the present document and most of the requirements have been adopted in the present document.

4.2.5 Project OASIS

The objective of OASIS is to define and develop an Information Technology framework based on an open and flexible architecture and using standards, existing or proposed by OASIS, which will be the basis of a European Disaster and Emergency Management system.

OASIS is intended to facilitate the cooperation between the information systems used by civil protection organizations, in a local, regional, national or international environment.
This Disaster and Emergency Management system aims to support the response operations in the case of large scale as well as local emergencies.

The following documents are relevant for requirements definition:

- OASIS User Requirements synthesis (D-TA2_01) [i.25].

- Definition of the OASIS Tactical Situation Object (D-TA2_06) [i.24]. The TSO provides the capability to exchange pieces of information, which participate to the Common Operational Picture. The TSO is focused on the definition of the format and semantic of the exchanged information, which is not the objective of the present document. TSO may be anyway useful for verification against a well defined operational scenario.

4.2.6 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 requirements definition:

- Users Requirements and First System Architecture Design (D2.1) [i.26]. This deliverable is strong influenced by the MESA requirements.

4.2.7 WIN

WIN is an Integrated Project partly funded by the European Comission's 6th framework program, under the priority 2.3.2.9 "Improving Risk Management".

WIN develops an interoperable info-structure that will be a major element of the future Single European Information Space for what concerns the environment and risk management.

The following documents are relevant for requirements definition:

- User Requirements Specifications (D3201) [i.27].

4.2.8 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.

The following documents are relevant for requirements definition:

Deliverables of WP 1 - User Requirements for Interoperability. This WP has the objective of capturing, with the contributions of the User Groups, the requirements for wireless interoperability, in order to understand the immediate challenges to solve for crisis management and multi-services cooperation in Europe (From WINTSEC DoW).

The WINTSEC project used also a questionnaire to end-users to collected information on their needs and requirements.

The WINTSEC project provided the following recommendations and considerations:

- One of the main challenges is still interoperability. Responders belonging to different agencies but in the same COI (Community of Interest) want to keep in contact during an operation, regardless of the network technology, the network coverage or different frequency bands.

- Voice is still the main requested service, followed by query to remote databases, weather and traffic information and images and video.

- Quality of service of voice is of paramount importance, especially in relation to difficult environments like underground or mountainous areas.

- Power consumption and battery life are considered important elements in long emergency crisis or natural disasters.

- The introduction of a new communication technology is very depended on economical consideration like the price of the handheld terminals or network infrastructure.

4.2.9 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 requirements definition:

- Survey of Use Cases. Deliverable 1.1-1 [i.28].
- User and System Requirements for Emergency Telecommunication Services. Deliverable 1.2-1 [i.29].

4.3 Others

4.3.1 GMDSS

The Global Maritime Distress Safety System (GMDSS) is an internationally agreed-upon set of safety procedures, services and communication systems used to increase safety and make it easier to rescue distressed ships, boats and aircrafts.

GMDSS should be considered in the definition of user requirements for the application of RRS in the sea/cost environment. For examples for Coastal Guard or Port Security applications

4.3.2 Search & Rescue

The activity of Search and rescue has the objective to locate access, stabilize, and transport lost or missing persons to a place of safety. Search and Rescue is one of the activities performed by public safety organizations. Search & Rescue is not internationally standardized but it is similarly implemented in various nations in the world.

An important technological support to search & rescue is the Cospas-Sarsat system, which is a satellite system capable of detecting distress alert transmissions from radio beacons that comply with Cospas-Sarsat specifications and performance standards, and determining their position anywhere on the globe. The collected distress alert and location data is then forwarded provided by Cospas-Sarsat Participants to the responsible SAR services.

The objective of the Cospas-Sarsat system is to reduce, as far as possible, delays in the provision of distress alerts to SAR services, and the time required locating a distress and providing assistance, which have a direct impact on the probability of survival of the person in distress at sea or on land.

For more details on the Coast-Sarsat systems, consult: http://www.cospas-sarsat.org.

The future European GNSS system will provide the *search and rescue* service, which is strong related to Cospas-Sarsat. The Galileo search and rescue component will provide two services. The Forward Link Alert Service, fully backward compatible with the current operational COSPAS-SARSAT components and interoperable with all other planned MEOSAR elements, detects activated distress beacons and notifies the appropriate rescue body. A novel service, known as the Return Link Service, will send a return message to the emergency beacon, notifying the emergency victims that their distress signal has been received and help is on its way.

It is recommended that an RRS-based communication system for Public Safety will support Cospas-Sarsat.

5 Input from the other TC RRS working groups

This clause describes the information and documentation produced by other TC RRS working groups (WG1, WG2 and WG3), which is relevant to the present document.

Functional Architecture (FA) in TR 102 682 [i.12] has described the requirements for the improvement of the utilization of spectrum and radio resources in reconfigurable radio systems and propose a generic architecture, namely the Functional Architecture (FA).

6 Public Safety Domains and Roles

6.1 Public Safety Domains

Public Safety organizations operate in a number of different domains, which have an impact on the definition of requirements for the equipment including communication systems.

The following main domains can be defined:

- Blue border

Identifies the border between land and sea or a major lake. We can make a distinction between a border included in a single political or governmental region (i.e. national context) and a border across different political or governmental regions (i.e. cross-national context). Because different public safety organizations are likely to operate in the second case interoperability requirements (see clause 9.1) may be more relevant.

- Green border

Identifies the border between two or more different political regions in the land. We can make a distinction between a border included in a single political or governmental region (i.e. national context) and a border across different political or governmental regions (i.e. cross-national context). Because different public safety organizations are likely to operate in the second case interoperability requirements (see clause 9.1) may be more relevant.

- Urban environment

Identifies an area in a city or a densely urbanized area. It has usually high density of people and buildings. Emergency crisis and other type of public safety scenarios in an urban environment is often characterized by a limited area of operation (300 m to few Kms), presence of man-made obstacles and need for a high reaction speed. Urban environment may have many facilities but traffic congestion may limit the mobility of Public Safety responders.

- Port or Airport

A port of airport has similar features to the urban environment as it is usually limited in size (few Km^2). In comparison to a generic urban environment, there is a larger presence of critical facilities (e.g. traffic control centre) which should be protected or whose services should be maintained. Critical facilities like deposit of dangerous materials like inflammable or chemical substances may also be present.

- Rural environment

Identifies an area, which is not densely urbanized like countryside, mountains, hills or forest areas. There may be natural obstacles like mountains and hills. An emergency crisis in a rural area may be quite large for the geographical extension (tens of Kms^2). A rural environment does not have usually an extensive communication infrastructure.

6.2 Public Safety Roles

Public Safety organizations are quite diversified both at national level and at European level. Their ranges of activities include all the areas related to the protection of the citizen and the public infrastructures. Public Safety organizations spans from volunteer organizations, which have received limited training to sophisticated para-military organizations (for example: the Carabinieri corps in Italy, which were historically king's army) and finally to defense organizations, which may be involved in large natural disaster scenarios like earthquakes.

One major challenge for the definition of a classification of Public Safety organizations at the European level is that similar organizations have different roles in different countries. This is, of course, due to the non homogenous historical development of public safety across Europe. This diversity is reflected in the different types of equipments and use of radio-frequency spectrum bands by public safety organizations. Operational procedures are also quite different, which is a major problem for border security organizations. This is not the case of other nations (e.g. USA), where similar studies have been attempted (see reference [i.4]).

Because of such diversity, the present document will not try to classify the various Public Safety organizations across Europe. The approach, adopted in the present document, is to define taxonomy of the main responsibilities and functions of public safety organizations.

The present document will then provide, for information purpose, a mapping of existing public safety organizations to defined functions and responsibilities.

For this purpose, the present document will use the information presented in the Statement of Requirements of Project MESA (see reference [i.3]).

The following functions are defined:

- Every day operations for Law Enforcement
- Emergency Medical and Health Services
- Border Security
- Protection of the environment
- Fire-fighting
- Search and rescue
- Emergency Crisis

These basic functions and the associated roles will be described in details in the following clauses.

In the present document, private organizations with similar structure and activities of public safety organizations will not be considered. For example private guard organizations of a business company.

6.2.1 Public Safety functions

6.2.1.1 Every day operations for Law Enforcement

This category includes the generic every day operations for Law Enforcement. Law enforcement is the function to prevent, investigate, apprehend or detain any individual, which is suspected or convicted of offenses against the criminal law. Law enforcement is a function usually performed by police organizations across Europe.

A number of sub-functions in this category can be defined:

- Tour of duty to identify and intervene in cases of offense to criminal law. This is also called patrolling.
- Criminal investigation.
- Customs verification, which are responsible for monitoring people and goods entering a country or to detect offense against customs law (this function is also shared by border security).
- Law enforcement in the transportation domain to identify law offenses on the transportation infrastructures like road, air, railways and sea.
- Custody and transportation of criminal convicts.

6.2.1.2 Emergency Medical and Health Services

NOTE: The following definition is extracted from [i.3].

The function of medical services is to provide critical invasive and supportive care of sick and injured citizens and the ability to transfer the people in a safe and controlled environment.

Doctors, Paramedics, Medical Technicians, Nurses or Volunteers can supply these services. They usually will also provide mobile units such as Ambulances and other motorized vehicles such as aircraft helicopters and other vehicles. The need for communications services for EMS providers inside and outside of the vehicles is vital in their work due to the fact they are nearly always in mobile resources that work in a wide variety of rural and metropolitan areas.

Information required by EMS providers includes:

- Patient Information

- Medical Information
- Resource Information
- Incident Information
- Geographical Information

Emergency medical and health systems should be able to inter-operate to provide a broad scope of services to all emergency medical staff to allow them to integrate with other agency systems.

The function of EMS includes also the function of "Disaster Medicine", which is the provision of triage, primary aid, transportation and secondary care in major incidents.

6.2.1.3 Border Security

Control of the border of a nation or a regional area from intruders or other threats, which could endanger the safety and economical well-being of citizens.

Border Security is usually performed by police organization or specialized border security guard. Coastal guard is a special case of border security.

The following sub functions can be defined:

- Verification of illegal immigration.
- Coastal guard.
- Verification of the introduction of illegal substances.
- Verification of introduction of goods in offense of customs laws.

6.2.1.4 Protection of the environment

This is the function to protect the natural environment of a nation or a regional area, including its ecosystems composed by animals and plants. This function is limited to the everyday operation of protecting the environment like monitoring of the water, air and land.

The specific function of fire fighting in described in a separate clause.

Forest guards, volunteers organizations or public organizations are usually responsible for this activity.

Protection of the environment does usually employ sensor devices and tools.

6.2.1.5 Fire-fighting

This is the function of putting out hazardous fires (see note) that threaten civilian populations and property. Hazardous fires can appear in urban areas (houses or buildings) or rural areas (forest fires).

NOTE: http://en.wikipedia.org/wiki/Fires

6.2.1.6 Search & Rescue

As described before, the activity of Search and rescue has the objective to locate access, stabilize, and transport lost or missing persons to a place of safety. Search and Rescue is one of the activities performed by public safety organizations.

6.2.1.7 Crisis Management

Crisis management integrates both search & rescue and emergency medical services and includes also the recovery of the essential flows related food, medicines, building material, electrical energy supplier, health and daily stuff, situation awareness and communication.

6.2.2 Applications

Future public safety communications applications will demand mobile broadband service, migrating from the current dominant voice-only mode to multimedia applications. In these applications large amount of data will be exchanged across the responders or between the responders and the central office. Because of the nature of Public Safety operations, such data is often transmitted by wireless communication. The objective of this clause is to provide an overview of the main current and future applications in public safety:

- Verification of biometric data. Public Safety officers may check the biometric data of potential criminals (i.e. fingerprints facial/iris recognition) during their patrolling duty. The biometric data could be transmitted in real-time to the headquarters or a centre with the biometric archives and the response could be sent back to the Public Safety officers. This would be a positive method of identification during field interrogation stops.

- Wireless video surveillance and remote monitoring. In these types of applications, a sensor (fixed or mobile) can record and distribute data in video-streaming format, which is then collected and distributed to public safety responders and command and control centres.

- Automatic number plate recognition where a camera captures license plates and transmits the image to headquarters or a centre with the plate data to verify that the vehicles have not been stolen or the owner is a crime offender.

- Documents scan. In patrolling or border security operations, public safety officers can verify a document like a driving license in a more efficient way. Documents scan is also useful in border security operations where people, who cross the borders, may have documents in bad condition or falsified.

- Database checks. This application area includes all the activities where public safety officers retrieve data from the headquarters to support their work.

- Location/Tracking for Automatic Vehicle/Officer Location. The public safety officer has a GNSS position localizer on the handheld terminal or the vehicular terminal. The positions are sent periodically to the headquarters so that the command centre can organized and execute the operations in a more efficient way.

- Transmission of Building/Floor plans and Chemical data. In case of an emergency crisis or a natural disaster, Public Safety responders may have the need to access the layout of the buildings where people may be trapped or where dangerous chemicals are kept. Chemical data, building or floor plans can be requested to the headquarters and transmitted to the public safety responders.

- Monitoring of Public Safety officer. Vital signs of Public Safety officers could be monitored in real-time to verify their health conditions. This is particularly important for firefighters at fireground incidents and officers involved in search & rescue operations.

- Remote emergency medical service. Through transmission of video and data, medical personnel may intervene or support the team in the field for an emergency patient.

- Sensor networks. Sensors networks could be deployed in a specific area and transmit images (thermal) or data to the Public Safety responders operating in the area or to the command centre at the headquarters. This application does not include video-surveillance, which is described above.

Table 1 provides an indication on what types of capabilities are needed by the application described above. The values are based on clauses 4.1.3, 4.1.4, 4.1.9, 4.2.4 and the questionnaire results from A.2.

The capabilities are mostly based to the definitions provided in clause 4.1.3:

- Throughput: data volume in a given time (could put numbers to this e.g. Kbps, Mbps, etc.).

- Timeliness: importance of the information arriving in an agreed space of time. Again, you could put numbers to this e.g. position information needs to be delivered within 5 seconds.

- Quality of Service: how reliable the information transmission needs to be. E.g. a bitmap image with some errors is still useable, a JPG image with some bit errors may be unreadable.

- Coverage. Geographical distance or range of the communication.

Table 1: Public Safety Applications

Application	Throughput	Timeliness	QoS	Coverage
Verification of biometric data	Medium	Low	High	Low
Wireless video surveillance	High	High	Medium	Low
Automatic number plate recognition	Medium	Medium	High	Medium
Documents scan	Medium	Low	Medium	Low
Database checks	Depends	Medium	Low	Medium
Location/Tracking for Automatic Vehicle/Officer Location	Low	High	Medium	High
Transmission of Building/Floor plans	Medium	Medium	Medium	Medium
Monitoring of Public Safety officer	Low	High	High	Medium
Remote emergency medical service	Medium	High	High	Medium
Sensor networks.	Medium	Medium/High	High	Medium/High

6.2.3 Public Safety organizations

Table 2 has the purpose to describe the most common types of Public Safety organizations. For each Public Safety organizations, we provide the type of equipment and applications, which are usually adopted by the organization.

In relation to the functions described in the previous clause, the table describes also the type of functions provided by each public safety organization.

NOTE: Some of the definitions are extracted from [i.3].

Table 2: Public Safety organizations descriptions and functions

Public Safety Organization	Description	Functions	Type of wireless communication Equipment
Police	The main objective of the police is law enforcement creating a safer environment for its citizen.	Law enforcement	Analog or digital professional mobile radio.
Fire Services	With variations from region to region and country to country, the primary areas of responsibility of the fire services include: • structure fire-fighting and fire safety; • wild land fire fighting; • life saving through search and rescue; • rendering humanitarian services; • management of hazardous materials and protecting the environment; • salvage and damage control; • safety management within an inner cordon; • mass decontamination.	Law enforcement, protection of the environment, search & rescue	Analog or digital professional mobile radio. Satellite communications. Avionic Communications.
Border Guard (Land)	Border Guard are national security agencies which performs border control at national or regional borders. Their duties are usually criminal interdiction, control of illegal immigration and illegal trafficking.	Border Security	Analog or digital professional mobile radio.
Coastal Guard	Coast Guard Services may include, but not be limited to, search and rescue (at sea and other waterways), protection of coastal waters, criminal interdiction, illegal immigration, disaster and humanitarian assistance in areas of operation. Coast Guard functions may vary with Administrations, but core functions and requirements are generally common globally.	Law enforcement, protection of the environment, search & rescue. Border Security	Analog or digital professional mobile radio. Avionic Communications Maritime Communications
Forest Guards	Type of police specialized in the protection of the forest environment. It supports other agencies in fire-fighting, law enforcement in rural and mountain environment.	Law enforcement, protection of the environment, search & rescue.	Analog professional mobile radio. Avionic Communications
Hospitals, field medical responders	The mission of the Emergency Medical Services (EMS) is to provide critical invasive and supportive care of sick and injured citizens and the ability to transfer the people in a safe and controlled environment. Doctors, Paramedics, Medical Technicians, Nurses or Volunteers can supply these services. They usually will also provide mobile units such as Ambulances and other motorized vehicles such as aircraft helicopters and other vehicles. The need for communications services for EMS providers inside and outside of the vehicles is vital in their work due to the fact they are nearly always in mobile resources that work in a wide variety of rural and metropolitan areas.	Search & rescue. Emergency Medical Services	In some cases, digital professional mobile radio. Commercial wireless systems (GSM, UMTS)
Military	Military is the organization responsible for the national defense policy. Because military is responsible for the nation protection and security, it may also supports public safety organizations in case of a large national disaster. Military organizations are very well equipped with many different wireless communication systems with high degree of security and reliability.	Search & rescue. Emergency Medical Services	A variety of military communications systems including avionic and maritime. They are usually equipped with a high level of robustness and security.
Road Transport Police	Transport police is a specialized police agency responsible for the law enforcement and protection of transportation ways like railroad, highways and others.	Law enforcement	Analog or digital professional mobile radio.
Railway Transport Police	Railway Transport police is a specialized police agency responsible for the law enforcement and protection of railways. In some cases, it is a private organization dependent on the railway service provider.	Law enforcement	Analog or digital professional mobile radio. In some cases, they use GSM-R terminals.

Public Safety Organization	Description	Functions	Type of wireless communication Equipment
Custom Guard	An arm of a State's law enforcement body, responsible for monitoring people and goods entering a country. Given the removal of internal borders in the EU, customs authorities are particularly focused on crime prevention.	Law enforcement	Analog or digital professional mobile radio.
Airport Security	Airport enforcement authority is responsible for protecting airports, passengers and aircrafts from crime.	Law enforcement	Analog or digital professional mobile radio. Avionic communication systems.
Port Security	Port enforcement authority is responsible for protecting port and maritime harbor facilities	Law enforcement	Analog or digital professional mobile radio. Maritime communication systems.
Volunteers Organizations or Civil Protection	Volunteer organizations are civilian with training on a number of areas related to Public Safety and environment protection. They voluntarily enter into an agreement to protect environment and citizens without a commercial or monetary profit.	Protection of the environment, search & rescue.	They are usually equipped with normal handset from the commercial domain and occasionally with analog or digital professional mobile radio.

7 Public Safety Use Cases and Operational Scenarios

7.1 Introduction

This clause describes public safety use cases on the operational scenarios which are relevant to the application of RRSs.

The applications of RRS will cover crisis management need to overcome situations produced by threats and to manage major events security respectively.

Any Uses Case will be described in order to make clear the operational, functional and performance requirements the RRS should be compliance to.

A classification of Public Safety operational scenarios have already been presented in the deliverables produced in the references described in clause 4.

One popular taxonomy is to classify the operational scenarios in:

- Citizen to citizen
- Authority to authority
- Authority to citizen
- Citizen to authority

Where authority or an authorized representative is an individual officer or institution authorized by public service (fire, police or health) to play a key role in handling of an emergency case (see ETSI EMTEL definitions in clause 4.1.3).

While this classification is quite useful to define the various flows of information among the participants to an operational scenario, it will be too generic for this context.

In the present document, we will adopt classification criteria similar to the one presented in Project MESA, where operational scenarios are classified along three dimensions.

In Project MESA, the classification criteria are Coverage, Environment and Situation.

In a similar way, in this context we will adopt the following dimensions:

- Geographical Extension. This dimension describes the size of the area involved in the emergency crisis.

- Environment Complexity. This dimension represents the complexity of the emergency crisis in terms of number of entities involved, difficulty of the environment and so on.
- Crisis Severity. This dimension represents the severity of the crisis.

The dimensions will be used to map the operational scenarios presented in the next clause.

The dimensions have a direct relation to the definition of the requirements. For example environment complexity has a direct impact to the requirements for interoperability as more participants will be participate to the scenario.

In a similar way, geographical extensions are directly correlated to the coverage, which are provided by the radio equipment.

7.2 Operational Scenarios

7.2.1 Routine Operations

This operational scenario of routine activity is where Law Enforcement Public Safety organizations, patrol their area of responsibility to identify law offenders.

The usage of the wireless communications is low in comparison to an emergency crisis.

While narrowband wireless communication services like voice or low data messaging has been the operational norm in this type of scenarios, the evolution of new applications requires an increase need for broadband connectivity to transmit images or video, which can be used to identify criminals.

7.2.2 Emergency Crisis

Emergency crisis includes various types of events due to intentional or unintentional causes, which create disruption to the normal business flow, may endanger life of civilians and destroy public or private facilities.

Examples of emergency crisis are:

- The London bombing of 7 July 2005. Reference [i.1] provides a very detailed and complete study on the application of cognitive radio systems in the resolution of this emergency crisis.
- A large fire of a building in an urban environment.
- An incident at a chemical plant.
- A large car or truck accident on a highway with presence of inflammable materials.
- A group of people has been kidnapped by criminal offenders.

An emergency crisis is usually an unplanned event.

Unless the emergency crisis has a direct impact on the communication infrastructure, communication services are not disrupted by their traffic capacity can overloaded because of the panic effect (as in the case of the London bombing).

7.2.3 Major Events

A major event is large planned event, which may involve a large number of people and organizations in a specific geographic area for a limited duration of time. A major event may also require a large number of resources both economical and organizational.

Examples of major event are:

- Concert.
- Political meeting.
- Sport event like a soccer championships or Olympics Games.

- A religious event.

Because of the large number of people involved and political/social elements, the risk for the security of the citizen is quite elevated.

Another consequence of the presence of a large number of people is the strain on the infrastructures, especially communication infrastructure, which is usually not sized for these types of event.

The communication infrastructure and its resources are therefore even more vulnerable to a crisis during the execution of a major event.

7.2.4 Natural disaster

A natural disaster is caused by natural phenomena (in opposition to an emergency crisis). The causes of a natural disaster continue in time for hours or days as in the case of a flooding or earthquake.

A natural disaster, which could require military participation, is usually a medium or large scale event, which affects a large regional area or an entire nation. The interoperability with military organizations adds a new level of complexity to the scenario as military personnel has usually higher levels of security and operational capability then public safety organizations.

Examples of natural disasters are:

- Earthquakes
- Large flooding
- Tsunami
- Large fire

The communication infrastructure and its resources are usually severely degraded or destroyed during a natural disaster. For this reason, the flexibility and interoperability of RRS technology could provide a benefit for radio communications and first-link establishment.

7.2.5 Search & Rescue

This type of scenario is related to the search and rescue of one or more person. It is usually conducted in a very isolated or difficult environment both due to difficult terrain or bad weather conditions. It is usually include a limited number of public safety organizations even if it may be a large scale event as in the case of a lost ship or airplane.

Example of search & rescue operations:

- A boat or a ship is lost in the sea or in a large lake.
- An aeroplane is lost in an isolated area.
- A mountaineer is lost in the mountains during a storm.

7.3 Mapping of operational scenarios along dimension criteria

This clause provides a mapping of the operational scenarios along dimension criteria. The mapping is only qualitative and is based on the references described in clause 2.1 and on the input provided by Public Safety organizations.

Table 3: Operational scenarios along dimension criteria

	Geographical Extension	Environment Complexity	Crisis Severity
Routine Operations	Low/Medium	Low	Low
Emergency Crisis	Low	Medium	High
Major Events	Low	High	Low
Natural Disaster	Medium/High	High	Medium/High
Search & Rescue	High	High	Low

7.4 Mapping among Public Safety organizations and operational scenarios

On the basis of the input of clause 2 and the results of the questionnaire described in Annex A: Questionnaire to Public Safety users, it is possible to provide information on how public safety organizations are present in the various public safety operational scenarios.

Table 4: Mapping of Public Safety organizations against operational scenarios

	Routine Operations	Emergency Crisis	Major Events	Natural Disaster	Search & Rescue
Police	High	High	High	Medium	Low
Fire Services	None	High	Medium	High	Medium
Border Guard (Land)	Low	Medium	Low	Medium	Medium
Coastal Guard	High	Medium	Low	Low/Medium	High
Forest Guards	Low	Low	Low	High	High
Hospitals, field medical responders	Low	High	Medium	High	Medium
Military	None	Low	Low	Medium	Low
Road Transport Police	High	Medium	Medium	Medium	Low
Railway Transport Police	Medium	High	Low	Low	None
Custom Guard	High	Low	Low	Low	None
Airport Security	High	Low	Medium	None	Low
Port Security	High	Low	Medium	Low	Medium
Volunteers Organizations	None	Medium	Medium	High	Medium

8 Benefits of the application of RRS to the Public Safety domain

Wireless communication scenarios are characterized by the coexistence of a variety of radio communication systems. Wireless networks differ from each other in the specific air interface technology, supported services, bit rate capabilities, coverage, mobility support, etc. Whilst different applications and needs have led to the deployment of such heterogeneous networks (e.g. commercial cellular systems, public-safety, etc.), all of them respond to society's fundamental demand for communications.

Wireless communications technologies play an essential role in emergency and disaster relief situations. Appropriate communications between first responders, authorities and citizens is crucial. It is generally acknowledged that existing wireless communication networks frequently fall short of meeting users' needs and consequently cannot properly support the management of these critical situations.

Even though the public safety community's technological needs have been understood for a long time, the capabilities of current public safety communications systems (e.g. Private Mobile Radio, PMR) are lagging behind some of the capabilities available in commercial mobile networks.

Some of the major limitations of public safety systems in emergency and disaster relief scenarios are:

- Lack of network capacity in emergency scenarios. Whilst in their day-to-day service the Network Operators may have learned to work around the shortcomings of their communication systems, the situation changes dramatically when an emergency causes additional stress for the system (and the operators). Emergency scenarios usually lead to exceptionally high traffic loads, that a single (e.g. PMR) wireless communication system may not be able to support. This situation can be worsened in scenarios with limited radio coverage (e.g. a traffic crash in a tunnel) or when parts of the communications infrastructure are damaged in the incident area.

- Lack of interoperability. The diversity of radio access technologies used by public safety organizations often creates technical interoperability barriers among different public safety agencies. As a result, first responders are frequently required to manage several separate (often incompatible) radio-communication systems. Furthermore, the political evolution of Europe has called for an increased collaboration among public safety organizations from different European countries. This has increased the need for harmonized procedures and interoperable technologies even more evident.

- Lack of support for broadband data rates. The evolution of public safety operations has created the need for applications as described in clause 6.2.2, where large amounts of data are exchanged between first responders or between the tactical front line responders and multi levels of a hierarchical command structure. Data-intensive multimedia applications have a great potential to improve the efficiency of disaster recovery operations (e.g. real-time access to critical data such as high resolution maps or floor plans).

Furthermore, emergency and disaster relief situations exhibit additional inherent challenges, which often impose severe difficulties on public safety communications. Examples of these are:

- The locations where emergency and disaster relief operations occur are unpredictable and the availability of communications facilities is not guaranteed in the incident area.

- Even if wireless communications infrastructure exists in the incident area, the first responders may not have the appropriate terminals.

- Public safety responders need wide area coverage, e.g. in the event of natural disasters like earthquakes or flooding, where a large area may be affected. Support for wide area coverage and higher transmission output is a conflicting requirement with low power consumption and extended battery life for handheld terminals.

- Public safety organizations operate in uncertain conditions and difficult environments both from a physical as well as from a radio propagation point of view, due to the presence of radio interferences or obstacles (man-made or natural).

- Public safety responders have special requirements regarding reliability, responsiveness and security of their communication systems.

Most of these challenges are at tactical level, for personnel involved in field-operations.

RRS technology can provide important benefits to resolve the limitation of existing public safety communication systems and resolve the challenges faced by public safety organizations.

NOTE: These topics are investigated in more detail in the present document, System Aspects.

Note that RRS technology does not imply that the existing public safety communication systems should be replaced. RRS can be used to augment the capabilities of existing systems. For example TETRA equipment can be enhanced with cognitive radio capabilities. More details on this aspect will be presented in the present document, System Aspects.

Lack of Network Capacity: The greater flexibility of RRS technology in comparison to conventional public safety communication systems can mitigate the problem of lack of network capacity during an emergency crisis.

Network capacity can be increased by implementing *spectrum sharing* or *network sharing.*

"Spectrum sharing" refers to either the possibility of managing radio frequency spectrum in a flexible way, such that both public safety and commercial communication services can be provisioned over the same frequency bands (e.g. allocate a public safety licensed band with mechanisms for interruptible spectrum leasing to commercial devices) or to sharing spectrum between different public safety license holders (e.g. spectrum pooling concept).

In spectrum sharing, RRS can be used to increase the use of spectrum during an emergency crisis by taking it from the commercial domain. In "normal" operational situations, Public Safety responders will not use the spectrum assigned to commercial providers. In "exceptional" situations like the ones described in clause 7, Public Safety RRS-based communication systems will reconfigure themselves to transmit in the commercial bands. When the "exceptional" situation is finished, the spectrum bands can be handed over to commercial providers. The increase of the spectrum is directly related to an increase in traffic capacity.

Spectrum sharing presents a number of challenges, which are not only at technical level, but they are mostly at procedural, organization and regulatory level:

- A clear definition of "normal" and "exceptional" operations to define when Public Safety organizations are authorized to use the spectrum assigned to commercial providers.
- Definition of the operational procedures to be established for switching the usage of the spectrum.
- Definition of the technical and operational mechanism to ensure that commercial domain will not use or transmit in the spectrum during "exceptional" situations. Otherwise, Public Safety communication systems will suffer from wireless interference by commercial providers.

There will be considerable resistance both from commercial providers, which will disagree on relinquishing spectrum resources (even for a short time) for which they have paid and by public safety organizations, which could be afraid of the increase of risk of QoS degradation in relation to "spectrum sharing". For more details on the issues and challenges of Spectrum Sharing, see TS 102 734 [i.13], System Aspects.

The capacity and efficiency of public safety communications networks can also be increased by implementing "network sharing" concepts with commercial networks in case of emergencies or natural or man-made disasters. "Network sharing" refers to the capability of sharing network resources like traffic capacity, communication services and broadband connectivity between networks, which have been designed for different tasks. In this case, Public Safety RRS-based networks could interoperate with commercial networks at the level of resource management.

This approach presents even more challenges than the spectrum sharing for the following reasons:

- Resource management interoperability between public safety networks and commercial networks is not standardized yet and there are significant differences between the two infrastructures.
- Resource prioritization is usually not implemented in commercial networks but it is an essential functionality requested by public safety networks.
- Definition of the operational procedures to be established for switching the use of the network resources.
- Public Safety and commercial networks have different levels of security for networks and resource management.

As in the case of spectrum sharing, there may be considerable resistance both from commercial providers, which would not like to give up the control of their network resources to an external party, and by public safety organizations, which would not like to give access, for security reasons, to their network to commercial provides.

Even with these challenges, both approaches should be taken in consideration.

In other domains like energy or water infrastructures, there are already existing procedures where public safety organizations can access and use resources of commercial providers in case of a natural disaster or an emergency crisis.

Interoperability: The European FPx projects WINTSEC and EULER have extensively investigated the application of RRS to remove the interoperability barriers across different radio access technologies (RAT). In both projects, the term Software Defined Radio (SDR) has been used.

Interoperability can be achieved by deploying software waveforms for each RAT on the terminal platform. To communicate through a specific RAT, the Public Safety responder can activate the related RAT waveform.

This solution has the disadvantage of increasing the price and the complexity of the handheld terminal and it may only be feasible on vehicular RRS or base stations RRS. Then, in this case, these latter RRSs should be able to perform multi and independent access technology so as to allow both commercial and professional terminals to operate only with their environment specific waveforms.

Broadband Connectivity: The capacity of providing broadband connectivity is not specific to RRS technology as any digital wireless communication systems with enough spectrum allocation can provide the broadband connectivity requested by Public Safety applications.

RRS technology can use the RF spectrum in a more efficient way than conventional wireless communication systems by implementing sophisticated cognitive radio algorithms which can adapt to changes in the environment.

RRS can provide the following additional benefits to the Public Safety organizations:

- **Upgradeability:** RRS are mostly based on software instead of hardware as conventional wireless communication system. As a consequence, it will be easier to replace elements of the radio.
  The ability to upgrade the communications system through a software download (even a remote download) provides a significant potential cost savings. Because the system can be upgraded without a substantial hardware change, new standards can be implemented more inexpensively and deployed on the RRS platform. An RRS-based network may be more expensive upfront but it will decrease significantly the operational and maintenance costs (low OPEX). This aspect can be summarized as the capability to allow "new technology insertion" with limited extra-cost, where "technology" here it stands for both HW components and access technologies.

- **Adaptability:** Thanks to their flexibility, RRS technology can adapt to the changing conditions of the environment. Some operational scenarios have a very dynamic nature with vehicles and personnel changing location and new organizations entering or exiting the context. RRSs can implement algorithms to sense the changes in the environment and adapt the transmission parameters like modulation, bandwidth and power in near real-time to establish or maintain connections with high QoS. RRSs nodes could also implement operational procedures in relation to a specific scenario through specific communication profiles. For example, in an urban scenario of limited geographical size, RRSs nodes could use a profile to increase the robustness to multipath fading and decrease the transmission power to limit power consumption.

- **Reconfigurability:** That is the capability to perform multi access technologies, they may be independent and simultaneous, but with integrated and not federated architecture able to share its HW and SW resources for its multi waveforms set. TETRA, V/UHF, WiMAX (that is broadband) and satellite are already current need for several Public Safety users.

A recap of the benefits of RRS technology for Public Safety is provided in figure 1:

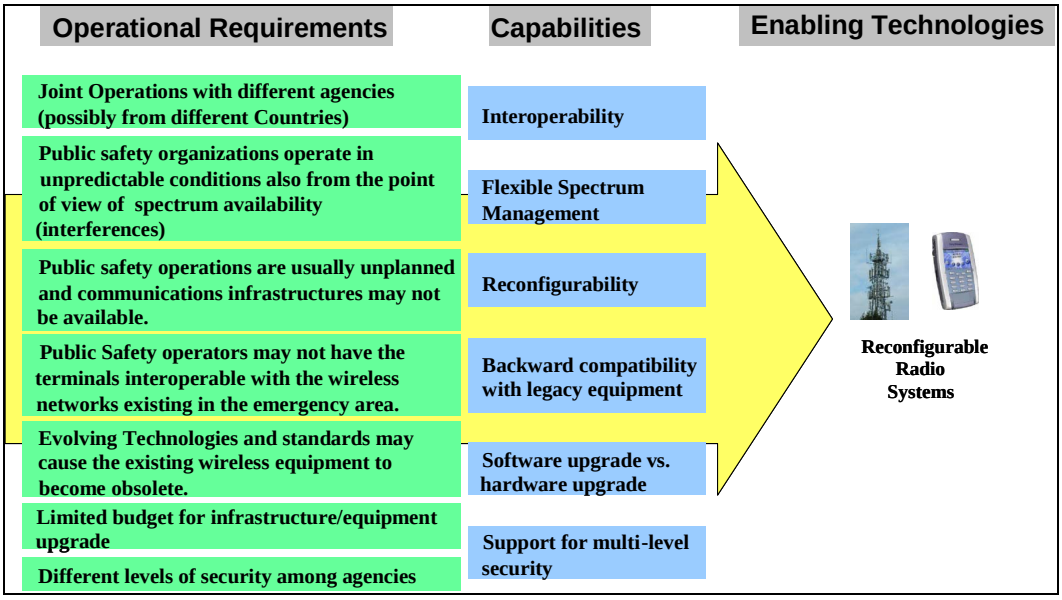


Figure 1: Benefits of RRS for Public Safety

9 Requirements Areas

This clause provides the list of requirements, which can be applied to the definition and application of RRS in Public Safety and Defense domain.

The requirements are grouped in requirements areas.

In relation to the operational scenarios defined in clause 7 some requirements are more or less relevant depending on the operational scenarios. A table at the end of the clause will describe the relevance of each requirement.

RRS-based systems should be able to provide a similar level of performance to the existing public safety communication systems like TETRA. As a consequence, communication networks based on RRS and which interoperate with TETRA, should be able to satisfy the same requirements defined for TETRA.

A similar concept applies to the other Radio Access Technologies (RATs) used in Public Safety.

As a consequence, this clause is focused on the specific requirements for the application of RRS to the Public Safety domain. Requirements specific to the RATs will not be considered in the present document unless they are used as a reference.

9.1 Interoperability

Interoperability is an essential requirement area because of the wide diversity of radio access technologies present in the Public Safety domain. Public Safety organizations use a number of different communication systems like TETRA, APCO 25, TETRAPOL, PMR and Satellite Communications and so on. A detailed list of the various communication systems is presented in TR 102 733 [i.14].

In this context, interoperability can be defined as the capability to communicate and distributed information across different wireless communications systems used by different public safety organizations. In general, interoperability refers to seamless operation between public safety responders using differing communication systems or products. For example, police, fire, and emergency medical services responding to an incident are interoperable when they can communicate with one another over otherwise incompatible wireless communication systems.

Interoperability barriers are present at different levels from a physical to an operational level.

Figure 2 provides an overview of the various communication levels and the interoperability barriers specifically for wireless communications.

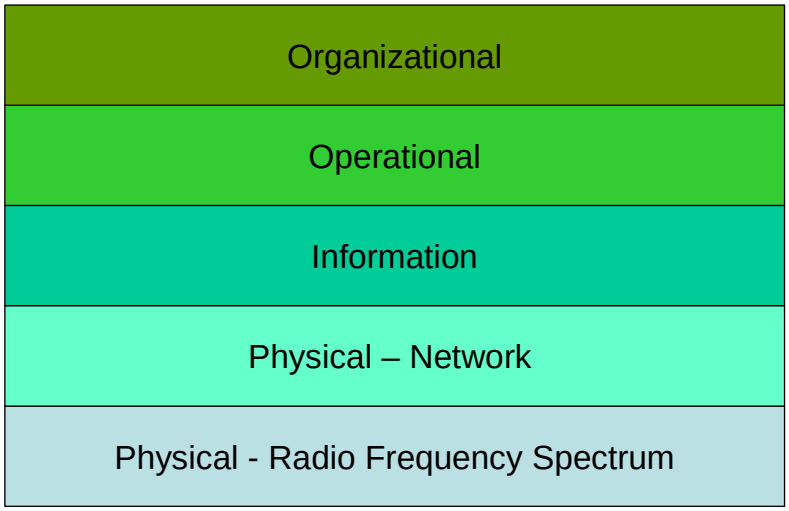


Figure 2: Interoperability levels in wireless communications for Public Safety

The interoperability levels are:

- Physical - Radio Frequency Spectrum. At this level, communication systems need to share the same radio frequency spectrum band in order to communication and being interoperable. For example, two users with different analog Professional Mobile Radio transmitting at different frequencies will not be able to communicate.
- Physical - Network. At this level communication systems should be able to communicate and distribute data using common protocols. For example, a user with TETRAPOL and a user with TETRA will not be able to communicate because of different protocols.
- Information. At this level, communication systems should be able to share information with similar content and format. For example, different communication systems should be able to exchange the information contents related to the physical layout of a chemical plant affected by a fire during an emergency crisis.
- Operational. At this level, public safety responders should be able to interoperate on the basis of established procedures. For example, different public safety organizations should have operational procedures to resolve together an emergency crisis.
- Organizational. At this level, public safety organizations should be able to interoperate. For example, contact points and hierarchies should be clearly defined.

The following detailed requirements can be defined in this requirements area:

- RRS should be able to transmit in the wide range of frequencies assigned to Public Safety bands. From 30 MHz to 1 GHz (or more in some specific European countries) on dedicated frequency slots.
- RRS should be able to interoperate and support the most common Public Safety. Commercial and Defense communication systems (or Radio Access Technologies) including TETRA, APCO 25, Analog PMR, GSM/UMTS, WiFi, WiMAX and Military communication systems.

In the case of RRS technology, an essential element is the capability to coexist with non-RRS communication systems.

This is the underlying principle for the following requirements:

- Support and interoperability with reconfigurable as well as non-reconfigurable terminals.
- Support and interoperability with reconfigurable as well as non-reconfigurable base stations.

- A RRS based system should be able to interoperate with non-RRS based system to provide emergency notifications to citizens during emergencies (see reference TR 102 182 [i.5]).

NOTE: RRS should be able to interoperate with non-RRS communication systems not only for direct voice or data communication but also for the management of communication resources including opening and closure of voice/data communications (see clause 9.6).

A specific case of interoperability is when a RRS system can act as a "bridge" between two different non-RRS communication systems. This capability is often called "relay", where voice or data information can be exchange or relayed through the RRS systems.

This is the underlying principle for the following requirements:

- RRS should be able to provide interconnectivity between two or more different non-RRS communication systems both for voice and data communications.
- RRS should be able to relay information like data messages between two or more different non-RRS communication systems both for voice and data communications.

9.2 Spectrum Usage

Public Safety wireless communication usage is characterized by a low usage pattern during routine operations and extremely high usage patterns during major disasters or events. Because traffic capacity is directly related to RF spectrum occupation, the consequence is that Public Safety organizations require a flexible approach to spectrum management to support their operational needs.

An important advantage offered by RRS radio system is to provide the needed flexibility and reconfigurability. RRS radio system can implement cognitive radio capability to implement a dynamic spectrum management approach.

The RRS radio system should be able to share spectrum resources in the same area with other radio networks. Spectrum sharing policies and etiquettes ensure that heterogeneous systems share the available resources in a fair manner.

In this requirements area, we can define the following detailed requirements:

- RRS should be able to adapt the transmission parameters like frequency bandwidth, frequency carrier modulation, power.
- RRS should be able to support flexible/dynamic spectrum assignment to network elements.
- RRS should be able to detect spectrum usage in the area. In other words, RRS should have spectrum sensing capability.
- RRS should be RF spectrum "aware" of the existence of other wireless communication systems transmitting in the area of operation.
- RRS should be able to exchange information on the use of spectrum usage with other RRSs in the coverage area.

Because RRS may be used by organizations with different levels of authority and operational priority (e.g. volunteers organizations have less priority than military), the RRS should have the means to avoid wireless interferences:

- RRS should be able to implement "mitigation" techniques to avoid or decrease the level of wireless interference to "licensed" or higher priority uses.

Allocation of spectrum bands for public safety is quite diversified across Europe. The same communication system may have different frequency bands assigned in different nations across Europe.

A strong benefit of RRS technology should be the capability to transmit in different frequency bands depending on the regulation context, where the RRS operate. This capability is particularly important in public safety operations in geographical areas with spectrum regulation different from where the public safety organization usually operates.

The following detailed requirements can be defined:

- RRS should be able to support communication for a RAT for different frequency bands.
- RRS should be able to dynamically change the operating frequency band depending on the context both operational and regional. For example, if a RRS system is moved, during an emergency crisis, from one regional area to another area, which uses a different allocation of RF spectrum bands, the RRS system should be able to reallocate its use of RF spectrum bands.

As described in clause 8, dynamic spectrum management has a number of technical and organizational challenges to be resolved before it can be applied to Public Safety domain. For example, the use of Cognitive Radio and Dynamic Spectrum Management may increase the risk of wireless interference and harmful coexistence between RRS or non-RRS wireless communication systems. For more details, see TS 102 734 [i.13], System Aspects.

9.3 Security

Public Safety domain has unique set of requirements for wireless communications in comparison to the consumer domain and defense 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, which should be protected. The safety of the human beings is dependent on the security and performance of wireless communications, which should guarantee integrity of the transmitted data being 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 Defense domain, it also presents unique challenges due to the broader range of participants (firefighters, medical support, volunteer organizations, …), each with its own level of security.

The following basic security functionalities should be provided:

- Authentication
  Public Safety users and their devices (terminals) should be authenticated. Authentication is the service to ensure that the communicating entity is the one that it claims to be.
- Access Control
  Access Control is used to guarantee that a resource (information or communication service) is used only by authorized users and to control under what conditions access can occur. Access Control includes authorization and accounting.
- Data Confidentiality
  To ensure that the data transmitted or stored in the wireless communication systems (including terminals and network) is protected from unauthorized disclosure.
- Data Integrity
  The communication networks will not allow unauthorized interception/modification of communications or information.
- Non-repudiation
  To protect against denial by one of the entities involved in a communication of having participated in all or part of the communication
- Availability
  To guarantee that the wireless communication resources are always available and usable by authorized users

For the specific case of RRS technologies, the following security functionalities should also be provided:

- Secure Software Download. RRS can download software and configuration files through the radio access interface. The software and configuration files may be needed to support interoperability with wireless communication not planned before the mission or to enhance the performance of the system. Secure software download can be quite complex to implement and it may increase the risk of security attacks especially if conducted during an operational scenario. One possibility would be to provide software download and upgradeability only to RRS base stations and not to handheld or vehicular terminals, but this may create mismatches in the network among terminals and base stations. It leads to the issue of what will happen to the "legacy" terminals communicating to a base station when the base station is reconfigured to a new mode. The recommendation is investigate secure software download in the standardization phase.

- Support for different levels of security including red (clear) network and black (encrypted) network. RRS-based systems may have the task to provide interoperability with many different communication systems and different users, each with its own level of security. This wide range 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 spectrum. The RRS wireless communication systems and terminals should guarantee interoperability without sacrificing the security of data in each network. Multi-level security can be quite complex to implement and it can dramatically increase the cost of RRS equipment. The recommendation is that multi-level security is provided only in few critical situations and on a limited number of communication nodes. One example is joint military-public safety operations where only the RRS nodes of the higher echelons of the chain of command have multi-level security capability.

9.4 Resilience

The RRS radio system should be particularly robust against change in the network topology or against wireless interferences, either intentional or unintentional.

A wireless communication system used in an emergency crisis is characterized by rapid changes in the context or the composition of the network. Natural or man-made obstacles may block or degrade the wireless signal. Nodes may leave or join the network. Wireless interferences could be created by damaged industrial, energy or communication infrastructures present in the area.

Connectivity between the network nodes should be maintained in a robust manner, and advanced protocols are required that reconnect nodes via different frequency bands.

In this requirements area, we can define the following detailed requirements:

- RRS should be able to change the transmission parameters to maintain the Quality of Service in the communication.

- RRS based wireless networks should be able to reconfigure themselves to recover from changes in the topology of the wireless network. Reasons for the topological changes can be based on the disappearance of an RRS node, presence of an obstacle which blocks the wireless communication path.

- RRS should be able to change the frequency band for transmission if that frequency band is impacted by wireless interference intentional or unintentional. Note that the geolocation of the source of interference is not considered a direct requirement of the RRS in the present document even if it could be implemented to validate the requirement described above.

9.5 Scalability

Public Safety operations are largely unplanned (apart from the case of a Major event). The RRS radio system should scales well with the number of users/nodes in the network.

RRS-based systems should be able to migrate their capabilities from normal everyday operations (routine operations) to unplanned events like emergency crisis in a specified time:

- A RRS based system should be able to support an increase of traffic capacity in a specified period of time.

- A RRS based system should be able to support an increase in the number of connected RRS and non-RRS wireless terminals in a specified period of time.

- A RRS based system should be able to support an increase in the use of radio frequency spectrum in a specified period of time.

9.6 Resource Management

This requirement area includes the requirements needed to support an effective management of the communication resources.

Because an emergency crisis involves many different types of public safety organization, an important capability is to support prioritization of the communication resources. Because emergency crisis is often a dynamic and changing environment, it is important that RRS provide this capability in a dynamic matter.

The following detailed requirements can be defined:

- Dynamic Prioritization. RRS nodes should be able to prioritize communication resources on the basis of the context or the type of users using a collaborative or non-collaborative approach.
- RRS should provide the capability of changing their transmission parameters (frequency and power) to decrease their level of power consumption.
- RRS should be able to set-up a communication resource or connection in a specific time. For example, voice communication should not be set-up in more than 300 ms and 500 ms in wide area operation. (This requirement is derived by [i.1]).
- Support of self-configuration of base stations. Self-configuration support includes means allowing real plug and-play installation of base stations and cells, i.e. the initial configuration including update of neighbor nodes and neighbor cells as well as means for fast reconfiguration and compensation in case of removal of cells and nodes and in failure cases.
- Support of self-optimization of the base stations. Self-optimization includes means allowing automated or autonomous optimization of the network performance w.r.t service availability, QoS, network efficiency and throughput.
- A RRS based system should be able to support different types of RRS terminals (handheld and vehicular).
- A RRS based systems should support the resource management protocols of non-RRS communication systems to cooperate on the allocation of de-allocation of communication resources both for RF spectrum and network.
- Seamless radio coverage throughout the whole area involved by the emergency crisis, including guaranteed availability of coverage also under exceptional conditions (see [i.1]).

One important feature of Public Safety communication systems is that they should provide service to their users for a long amount of time without recharging. This feature is particularly important in the case of emergency crisis or natural disaster, which have a long duration.

This feature is also important in the emergency crises, which are related to a large geographical area as the need to support a large coverage may increase power consumption.

RRS has the promise to increase the efficiency in power consumption.

The following requirement applies:

- RRS should provide the capability to control and optimize energy power consumption. For example, RRS may use their spectrum sensing capability to automatically regulate their transmission power.

RRS-based technology should provide the same security capabilities for resource management like existing public safety communications systems (i.e. TETRA). For example, the capability of blacklist a terminal or base stations or remove a subscriber.

The following requirements apply:

- RRS should provide the capability to blacklist a terminal.
- RRS should provide the capability of adding/removing a subscriber.

9.7 Operational support and Usability

This clause describes the requirements area to support or improve the operational capability of Public Safety responders.

In opposition to the commercial domain, Public Safety organizations have well defined organization and procedures, which should be supported by the public safety communication systems.

RRS should be able to support the implementation of operational procedures. For example change of the transmitting parameters in response to a change in the operational scenario.

The following requirements can be defined:

- RRS should be able to provide group communications among the members of a Community of Interest (COI).
- RRS should be able to provide Direct Mode of Operation (DMO) without a base station or a fixed wireless infrastructure.
- RRS should provide the capability to create mobile ad-hoc networks with or without a base station or a fixed wireless infrastructure.
- RRS should be able to support the implementation of operational procedures. For example change of the transmitting parameters in response to a change in the operational scenario.
- RRS should be able to provide broadcast communications.
- The impact of the introduction of RRS technology to Public Safety organizations and procedures should be minimized.

9.8 Mapping of requirements areas against operational scenarios

The purpose of table 5 is to show the relevance of each requirements area against the operational scenarios. The table is based on feedback from Public Safety users and the input from the references described in clause 2.2.

Table 5: Mapping of requirements areas against operational scenarios

	Patrolling for Law Enforcement	**Emergency Crisis**	**Major Events**	**Natural Disaster**	**Search & Rescue**
Interoperability	Low, as it is eventually necessary for border monitoring.	High, as it needs to cooperate adopting common operational picture description and other common policies.	High, as it needs to assure information flow among different policy forces and headquarters.	High, as it needs to cooperate adopting common operational picture description and other common policies.	Medium, as it is eventually necessary for international S&R missions.
Spectrum Usage	Low, as routine operations do not need high spectrum usage.	High, as it needs additional bandwidth and traffic capacity.	High, as it needs additional bandwidth and traffic capacity.	High, as it needs additional bandwidth and traffic capacity.	Low, as this scenario is characterized by few stakeholders and large geographical areas.
Security	Medium.	High, as there may be present many vulnerabilities and potential attackers.	High, as there are many different organizations with various levels of security.	High, as there may be present many vulnerabilities and potential attackers.	Low, as there is a low probability for a security attack.

	Patrolling for Law Enforcement	Emergency Crisis	Major Events	Natural Disaster	Search & Rescue
Resilience	Low as network infrastructure should be fully operational.	High as the network infrastructure may be degraded or present vulnerabilities.	Medium as the network infrastructure may be vulnerable to attacks but it should be fully operational.	High as the network infrastructure may be degraded or present vulnerabilities.	Medium, as availability is a very important requirement but the network infrastructure should be fully operational.
Scalability	Low as routine operations are well planned in terms of resource and traffic needs.	High as it needs additional bandwidth and traffic capacity.	High as it needs additional bandwidth and traffic capacity.	High as it needs additional bandwidth and traffic capacity.	Low, as there is no need for increased traffic capacity.
Resource Management	Low as routine operations are well planned in terms of resource and traffic needs.	High as prioritization of the resource is critical in emergency crisis.	Medium, as prioritization of resource is important but not like in the case of emergency crisis and natural disasters.	High as prioritization of the resource is critical in natural disasters.	Low.
Operational support and Usability	Medium as it will improve the speed response of public safety officers.	High as it needs high usability and operational support to resolve the crisis.	Medium as the size of the event requires a good operational support but not as in the case of emergency crisis and natural disaster.	High as it needs high usability and operational support to resolve the natural disaster.	Medium.

9.9 Parameters/metrics for requirements evaluation and prioritization

From the requirements defined in the previous clauses, is possible to extract metrics, which can be used to measure the performance of RRS based systems.

The following metrics can be defined:

- Connection Setup Time. This is time needed to setup a voice connection or a data connection.
- Time for delivery of messages. This is the time requested to successfully deliver a message from one wireless terminal to another.
- Number of dropped connections. The number of dropped connections occurred in a specific time.
- Robustness against external interferences or security attacks. This parameter measures the level of degradation of a connection in presence of a wireless interference. The degradation can be calculated as Error Vector Magnitude (EVM) or Bit Error Rate (BER). The performances at user level are preferred, like information degradation, voice interruption and data lost.
- Data throughput in relation to the number of users. This parameter measures the scalability of the system in terms of traffic capacity.
- Power Consumption. This parameter measurement the efficiency of the RRS system in terms of power consumption.
- Coverage. This parameter measures the extension of the overall RRS system.

Annex A:
Questionnaire to Public Safety users

A.1 Questionnaire format

The purpose of this annex is to describe the contents and the results of Questionnaire distributed by ETSI TC RRS WG4 to end-users across Europe.

The questionnaire is composed by two sections or worksheets:

1) In the first worksheet are requested information about the identity, communications, capabilities and the most common applications used by the end users.

Respondent Profile			
Name			
Last Name			
Agency			
Please indicate your affiliation by ticking **only one** of the boxes below that best matches your organization/business			
If your affiliation is not listed please write it in the space provided in the "other" box and tick the box accordingly			
User Organization			
Police			
Fire Services			
Border Guard (Land)			
Coastal Guard			
Forest Guards			
Emergency Medical Services (EMS)			
Military			
Transport Police			
Custom Guard			
Airport Security			
Volunteers Organizations			
Other			
Question 1			
Which type of wireless communication system are you using?			
Insert multiple choices if needed.			
TETRA			
TETRAPOL			
APCO25			
WiFi			
WiMAX			
Analog Professional Mobile Radio			
GSM			
GPRS			
UMTS			
Satellite Network			
ZigBee			
Bluetooth			
Other			
Question 2			
Do you plan to enhance your existent radio communication system in the near future (within 3-5 years)?			
Yes			
No			
If yes, which systems (just a description)			
Question 3			
What type of services are you using?			
Voice			
Data			
Messaging			
Other			
Question 4			
If your systems supports data communications, please briefly describe what kind of services are transmitted via the network in your current operations.			

Single Voice calls (two speakers)			
Group Voice calls			
Short text messages (like SMS)			
Access to database (data query)			
Access to web			
Video		Yes	
Video Conferencing		No	
Images, scene photos			
Building or facilities plans			
Medical information			
Biometric data (for example on suspected criminals)			
Hazardous materials information			
Weather, traffic information			
Inventories			
Other types of data files			
Question 5			
If your systems supports data communications, please briefly describe what kind of services you consider essential for mission critical applications?			
Single Voice calls (two speakers)			
Group Voice calls			
Short text messages (like SMS)			
Access to database (data query)			
Access to web			
Video		Yes	
Video Conferencing		No	
Images, scene photos			
Building or facilities plans			
Medical information			
Biometric data (for example on suspected criminals)			
Hazardous materials information			
Weather, traffic information			
Inventories			
Other types of data files			
Question 6			
Do you have surveillance sensors connected to the communication networks?			
Yes			
No			
Question 7			
What type of frequency bands are you using? (for example 400-440 MHz)			
Question 8			
Are you sharing the network with some other user?			
Yes			
No			
Question 9			
During field operations, do you often need to interoperate with other organizations listed above?			
Yes			
No			
Question 10			
Specifically, during field operations, do you interoperate with military organizations?			
Yes			
No			
Question 11			
Your networks are composed by how many base stations (rough figure)?			
Question 12			
You networks are composed by how many handset terminals (rough figure)?			
Question 13			
You networks are composed by how many vehicular terminals (rough figure)?			
Question 14			
Operational Scenarios			
Which operational scenarios are you usually involved? Multiple choices. Please, consult glossary sheet for definitions			
Police Normal Operation (Urban Environment)			
Police Normal Operation (Rural Environment)			
Police Escorting (Urban Environment)			
Fire Accident (Urban Environment - large building)			
Fire Accident (Urban Environment - residential)			
Fire Accident (Rural - Forest area)			
Fire Accident (Industrial Facility)			
Fire Accident (Marine environment)			
Border Security (criminal interdiction) - Land			

Border Security (criminal interdiction) - Coast			
Border Security (control illegal immigration Land)			
Border Security (control illegal immigration Coast)			
Search & Rescue (Land)			
Search & Rescue (Maritime)			
Airport Security crisis			
Port Security crisis			
Medical Support (urban)			
Medical Support (rural)			
Major Event (concert, soccer match)			
Natural Disaster (earthquake)			
Emergency crisis (urban)			
Emergency crisis (rural)			
Emergency crisis (coastal)			
Road Transportation crisis			
Railway Transportation crisis			

2) The second worksheet has the objective to collect information on the most important enhancements requested by public safety communication end-users from next generation public safety communication technologies including cognitive radio and dynamic spectrum management.

The format is based on the allocation of "currency" units, which can be used to highlight the most important enhancements.

NOTE				
You have been provided with an imaginary 400 units of currency for the possible enhancement areas listed under each of the 4 category questions below. You can spend 100 units of currency on each specific area distributing the unit points among the listed items. One example is listed below. Units cannot be reused across areas.				
Question 1			**Question 2**	
	Spend			**Spend**
What are the most important enhancements for your organization from an operational point of view?			**What are the most important enhancements for your organization from an economic point of view?**	
Broadband connectivity			Decreased cost of network infrastructure including base stations	
Wireless interoperability with other safety agencies			Decreased cost of vehicular terminals	
Improved reliability of the wireless network			Decreased cost of handheld terminals	
Capability of using existing commercial network systems (for example: GSM/UMTS)			Improved upgradeability of the terminals (BS, vehicular, handheld) to new communications standards. Cost reduction in upgrading terminals.	
Increased user mobility			Energy efficiency during operations. Decreased power consumption.	
Avoid to use multiple terminals			Other	
Improved communications underground/tunnel			Other	
Capability of creating local wireless networks.			Other	
Improve roaming across region or countries			Other	
Other			Other	
Other				
TOTAL	0		**TOTAL**	0
	100		**Total**	**100**
Question 3			**Question 4**	
	Spend			**Spend**
Broadband data communications. Which type of data communication you would like to be enhanced?			**Functional Enhancements**	
Messages of large size (greater than 100 KByte)			Increased RF coverage	
Access to database (data query)			Increased traffic capacity	
Access to web			Increased Grade of Service (GoS)	
Video			Increased frequency efficiency	
Video Conferencing			Increased robustness again wireless interferences	
distribution of images, scene photos			Increased voice quality	
Building or facilities plans			Increased data throughput	
Medical information			Increased security of voice and data	
Biometric data (for example on suspected criminals)			Decreased time for call setup	
Weather, traffic information			Other	
Software terminal upgrades in real-time			Other	
Other			Other	
Other			Other	
Other				
Other				
TOTAL	0		**TOTAL**	0
	100			**100**

A.2 Questionnaire results

The questionnaire was distributed to a large number of end-users organizations of various types across Europe. The results of the questionnaire were discussed at the Workshop on Dynamic Spectrum Management and Cognitive Radio for the Public Safety at the Joint Research Centre of the European Commission in Italy (http://sta.jrc.ec.europa.eu/).

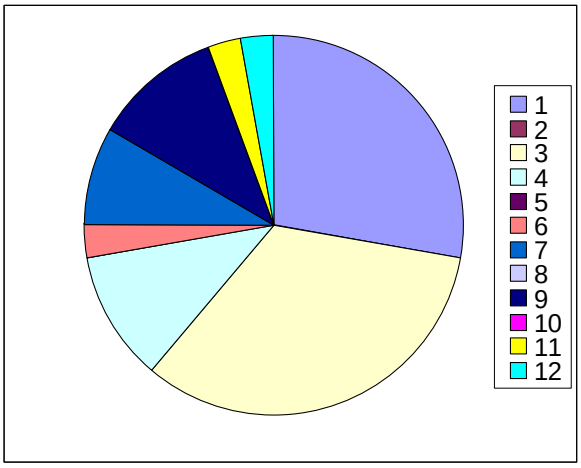
Twenty five responses were received and they have been used to produce the following charts.

NOTE: In some cases, the questionnaire allowed multiple choices. For example, a public safety organization may use more than one communication system.

The results are the following:

Types of Public Safety organizations.
The following chart shows the composition of the public safety organizations, which participated to the questionnaire.

As the reader can see, the majority were Police and Border Guard.



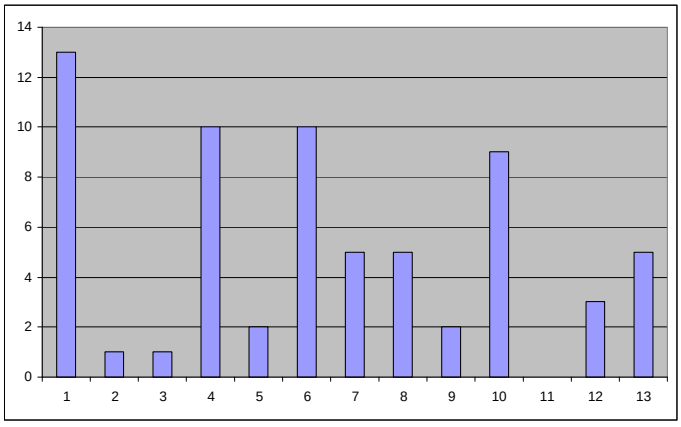
1	Police
2	Fire Services
3	Border Guard (Land)
4	Coastal Guard
5	Forest Guards
6	Emergency Medical Services (EMS)
7	Military
8	Transport Police
9	Custom Guard
10	Airport Security
11	Volunteers Organizations
12	Other

Figure A.1: Distribution of Public Safety organizations

Current types of communication

The following chart shows the breakdown of the types of communications systems used by the public safety organization.

The majority of the communication systems are TETRA and Analog PMR. It is interesting to see that many public safety organizations are using commercial systems like WiFi, GSM, GPRS and UMTS. Most of the communication systems declared in the other category are VHF maritime and avionics, which are mostly used by costal guard organizations.



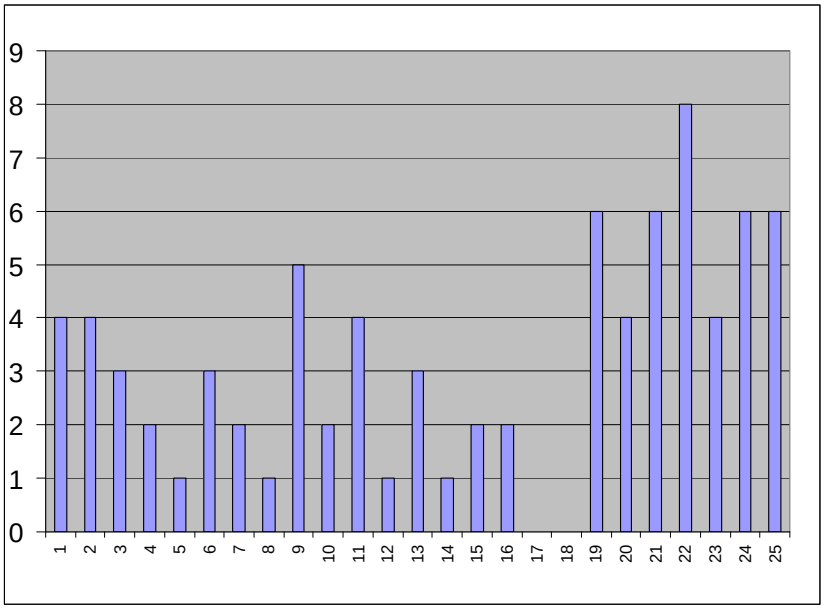
1	TETRA
2	TETRAPOL
3	APCO25
4	WiFi
5	WiMAX
	Analog Professional
6	Mobile Radio
7	GSM
8	GPRS
9	UMTS
10	Satellite Network
11	ZigBee
12	Bluetooth
13	Other

Figure A.2: Distribution of communication systems used by Public Safety organizations

Operational Scenarios

The following chart shows the types of operational scenarios where public safety organizations operate.

Because Emergency Medical services did not participate to the questionnaire, there is not feedback on elements 17 and 18.



1	Police Normal Operation (Urban Environment)
2	Police Normal Operation (Rural Environment)
3	Police Escorting (Urban Environment)
4	Fire Accident (Urban Environment - large building)
5	Fire Accident (Urban Environment - residential)
6	Fire Accident (Rural - Forest area)
7	Fire Accident (Industrial Facility)
8	Fire Accident (Marine environment)
9	Border Security (criminal interdiction) - Land
10	Border Security (criminal interdiction) - Coast
11	Border Security (control illegal immigration Land)
12	Border Security (control illegal immigration Coast)
13	Search & Rescue (Land)
14	Search & Rescue (Maritime)
15	Airport Security crisis
16	Port Security crisis
17	Medical Support (urban)
18	Medical Support (rural)
19	Major Event (concert, soccer match)
20	Natural Disaster (earthquake)
21	Emergency crisis (urban)
22	Emergency crisis (rural)
23	Emergency crisis (coastal)
24	Road Transportation crisis
25	Railway Transportation crisis

Figure A.3: Operational scenarios

Replacement plan

The majority of public safety organizations would like to replace their network infrastructure in the next 3-5 years.

14 organizations plan to change the network against 11 organizations, which do not plan to upgrade it.

The majority of the organization, which plan to change the network, will deploy TETRA technology.

Interoperability with military organizations

The data was incomplete as many users did not specify if they interoperate with military organizations. The partial data is that half of the organizations do not interoperate with military organizations.

Sensor Networks

18 Public Safety organizations stated that they do not have sensor networks connected to the communication infrastructure against 7 organizations, which have a connected sensor network.

Basic Services

The breakdown of the basic services (voice, data, messaging) used by the Public Safety organizations is:

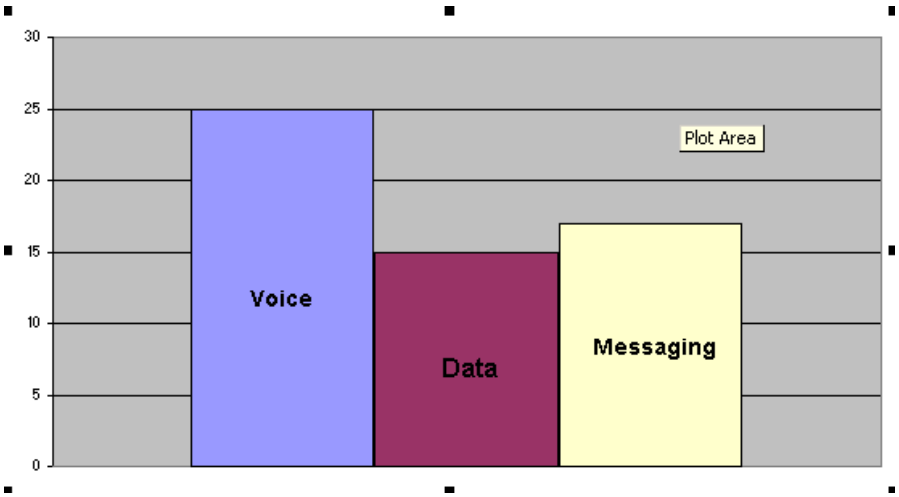


Figure A.4: Basic Services

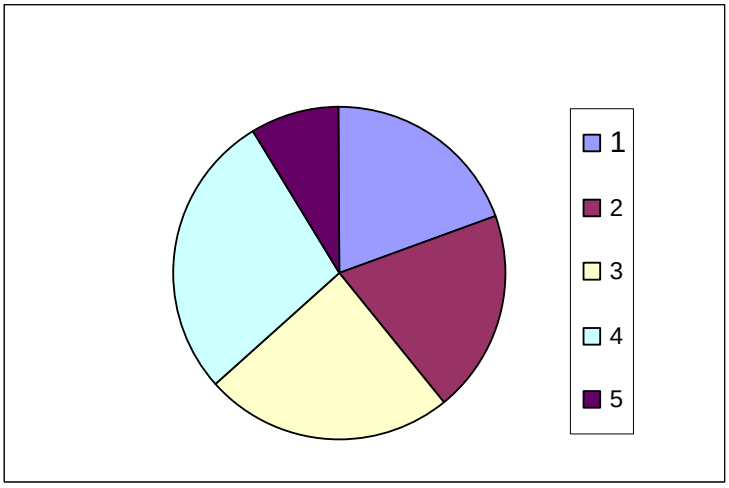
Operational Enhancements

The majority of the Public Safety organizations would like an enhancement of broadband connectivity followed by improved reliability and improved roaming functionality.

1	Broadband connectivity
2	Wireless interoperability with other safety agencies
3	Improved reliability of the wireless network
4	Capability of using existing commercial network systems (for example: GSM/UMTS)
5	Increased user mobility
6	Avoid to use multiple terminals
7	Improved communications underground/tunnel
8	Capability of creating local wireless networks.
9	Improve roaming across region or countries
10	Other
11	Other

Economic Enhancements

There was not a clear majority on the preference for economic enhancement, even if the improved upgradeability of the terminals is an important factor.



1	Decreased cost of network infrastructure including base stations
2	Decreased cost of vehicular terminals
3	Decreased cost of handheld terminals
4	Improved upgradeability of the terminals (BS, vehicular, handheld) to new communications standards. Cost reduction in upgrading terminals.
5	Energy efficiency during operations. Decreased power consumption.

Figure A.5: Economic Enhancements

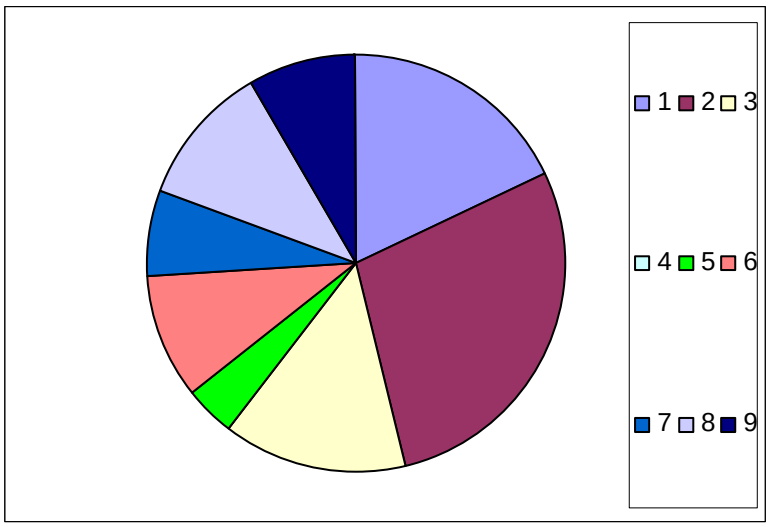
Broadband connectivity Enhancements

The needs for broadband connectivity is mostly driven by messaging service for large messages (1), video streaming (4) and access to database (2). Videoconferencing was not considered an important service.

1	Messages of large size (greater than 100KByte)
2	Access to database (data query)
3	Access to web
4	Video
5	Video Conferencing
6	distribution of images, scene photos
7	Building or facilities plans
8	Medical information
9	Biometric data (for example on suspected criminals)
10	Weather, traffic information
11	Software terminal upgrades in real-time

Functional Enhancements

Improvement of traffic capacity is the most requested enhancement, followed by increased RF coverage and improvement of Grade of Service (GoS).



1	Increased RF coverage
2	Increased traffic capacity
3	Increased Grade of Service (GoS)
4	Increased frequency efficiency
5	Increased robustness again wireless interferences
6	Increased voice quality
7	Increased data throughput
8	Increased security of voice and data
9	Decreased time for call setup

Figure A.6: Functional Enhancements

History

Document history		
V1.1.1	October 2009	Publication