JRC Scientific and Technical Reports

# Report of the workshop on "Interoperable communications for Safety and Security"


Workshop jointly organized by DG ENTR and DG JRC with the support of EUROPOL and FRONTEX.

Gianmarco Baldini

28-29 June 2010 – Ispra, Italy
EUR 24540 EN

JRC
EUROPEAN COMMISSION

ipsc
Institute for the Protection and Security of the Citizen

The mission of the JRC-IPSC is to provide research results and to support EU policy-makers in their effort towards global security and towards protection of European citizens from accidents, deliberate attacks, fraud and illegal actions against EU policies.

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information: Gianmarco Baldini
Address: Via E. Fermi 2749, I-21027 Ispra (VA), Italy
E-mail: gianmarco.baldini@jrc.ec.europa.eu
Tel +39 0332 786618
Fax +39 0332 785469

http://ipsc.jrc.ec.europa.eu/
http://www.jrc.ec.europa.eu/

Legal Notice
Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of this publication.

Europe Direct is a service to help you find answers
to your questions about the European Union

Freephone number (*):
00 800 6 7 8 9 10 11

(*) Certain mobile telephone operators do not allow access to 00 800 numbers or these calls may be billed.

A great deal of additional information on the European Union is available on the Internet.
It can be accessed through the Europa server http://europa.eu/

JRC60381

EUR 24540 EN
ISBN 978-92-79-16921-2
ISSN 1018-5593
doi:10.2788/19075

Luxembourg: Publications Office of the European Union

© European Union, 2010

Reproduction is authorised provided the source is acknowledged

Printed in Italy

# Table of Contents

# Abbreviations

AP Access Point
APCO Association of Public-Safety Communications Officials International
API Application Program Interface
CEPT European Conference of Postal and Telecommunications Administrations
CPC Cognitive Pilot Channel
CR Cognitive Radio
CS Circuit Switched
DMO Direct Mode of Operation
DSM Dynamic Spectrum Management
ECC Electronic Communications Committee
EDA European Defence Agency
ESRA European Software Radio Architecture
ESRAB European Security Research Advisory Board
ESRIF European Security Research and Innovation Forum
GSM Global System for Mobile communications
HF High Frequency
HSD High Speed Data
HW Hard Ware
LTE Long Term Evolution
PMR Professional Mobile Radio
PPDR Public Protection and Disaster Relief
QoS Quality of Service
RRS Reconfigurable Radio Systems
RSPG Radio Spectrum Policy Group
RTOS Real Time Operating System
SCA Software Communications Architecture
SDR Software Defined Radio
SW Soft Ware
TDMA Time Division Multiple Access
TETRA TErrestrial Trunked Radio
UHF Ultra High Frequency
UMTS Universal Mobile Telecommunications System
VHF Very High Frequency
WF Waveform

# Definitions

**N**ote: all definitions are from ETSI unless specified.

**Broadband:** communication service providing data rates higher than wideband (typically above 1 Mbit/s)

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

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

**DMO:** mode of simplex operation where mobile subscriber radio units may communicate using radio frequencies which may be monitored by, but which are outside the control of, the TETRA V+D network. DM operation is performed without intervention of any base station.

**IP:** standard protocol designed for use in interconnected systems of packet-switched computer communication networks.

**Mission critical situations:** situations where human life, rescue operations and law enforcement are at stake

**Narrowband:** communication service providing data rates up to about 100 kbit/s

**Public safety organization:** organization which is responsible for the prevention and protection from events that could endanger the safety of the general public
NOTE: Such events could be natural or man-made. Example of Public Safety organizations are police, fire-fighters and others

**Public Protection Disaster Relief (PPDR):** The term 'Public Protection' is used to describe critical public services that have been created to provide primary law enforcement, fire fighting, emergency medical, and disaster recovery services for the citizens of the political sub-division of each country. These individuals help to ensure the protection and preservation of life and property. Note that the term Public Safety and Disaster Response, within certain regions, can also be construed as PPDR. (from Project MESA TR 170 002 V3.1.1).

**Wideband**: communication service providing higher data rates than narrowband (typically hundreds of kbit/s).

**Wireless Sensor Networks:** A Wireless Sensor Network (WSN) is a special type of ad hoc network composed of a large number of nodes equipped with different sensor devices. Sensor Networks may enable novel applications that are related to different areas such as environmental monitoring, industrial and manufacturing automation, health-care, and military. Commonly, wireless sensor networks have strong constraints regarding power resources and computational capacity.

# 1. Introduction

Public Protection and Disaster Relief (PPDR) services bring value to society by creating a stable and secure environment. The provision of adequate capabilities to PPDR organizations and its officers is a priority subject for citizens, National Governments and the European Union.

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

Telecommunications technologies provide the capability of exchanging information (e.g. voice or data) to connect all the involved parties in the crisis and to coordinate the relief efforts.
In the field, wireless communications have an essential role to support the mobility of first time responders by providing continuous connectivity among responders and with the headquarters.

Wireless communications can support first time responders in a variety of operational tasks including:

- Maintain voice communication to coordinate the relief efforts for the resolution of the crisis.
- Creation and distribution of a Common Operational Picture among all the responsible parties.
- Collect and distribute data on the operational context or the environment from sensors.
- Retrieve data from central repositories (e.g. building plans, inventory data) to support their activity.
- Support the tracking and tracing of the supply chain of goods and materials needed in the response and recovery phases of a crisis.

To support these tasks, telecommunications must be reliable, secure and provide minimal levels of Quality of Service (QoS). Misinterpretations can cause loss of life or delay the resolution of the disaster.

In Europe, many dedicated network infrastructures have been built and deployed to provide the necessary capabilities for PPDR organizations. There are still a number of challenges to be resolved through the combined efforts of government, industry, end-users and research.

On the 28th and 29th June 2010, DG ENTR together with DG JRC and with the support of EUROPOL and FRONTEX has organized a workshop to identify the main challenges in the European PPDR context and describe the research activities to address and resolve

such challenges. Regulations and standardization play an important role in applying the results of research to the market and to the PPDR end-users.

The Workshop was called to reflect widespread comment that lack of interoperability was limiting the effectiveness of PPDR practitioners in actual operations, and an evident lack of understanding as to whether these limitations arose from technology, operational procedures, gaps in procurement or research. The aim of the workshop was to bring clarity to the interoperability needs and limitations and help participants develop their strategies for future improvements.

The workshop has seen a large participation of representatives from the government, standardization, industry and PPDR end-users.

The workshop has identified research gaps and it has defined a number of recommendations, where action at European level should be taken.
The purpose of this report is to describe the findings of the workshop and the related recommendations.

The report is structured in the following sections:

- Section 2 presents an analysis of the current challenges for PPDR communications and "state of art" on the current initiatives in Europe and the world.
- Section 3 provides a report on the workshop and the related presentations.
- Section 5 highlights the main observations and elements from the workshop.
- Section 6 identifies and describes the recommendations for regulations, research and standardization.

The report is complemented by the following annexes:

- Annex A provides a description of the Public Safety organizations and their functions.
- Annex B provides a description of the current and future applications, which can drive the evolution of Public Safety communications.
- Annex C provides a description of the research areas and technologies discussed in the report.

Note: while PPDR is the term used in the report, some presenters have chosen to use the term Public Safety in their presentations.

# 2. Analysis of challenges and research gaps for PPDR communications

## 2.1. Challenges for PPDR communications

In recent years, the capabilities of PPDR organizations across Europe have been considerably improved with the deployment of new technologies including dedicated TETRA and TETRAPOL networks and a range of new sensors (e.g. biometric identification). Nevertheless, a number of events like the London bombing of 7th July 2005, the Schiphol airport disaster and the flooding disasters in 2010 have highlighted a number of challenges for PPDR organizations.

The following challenges have been discussed and presented at the workshop:

- **Interoperability**. Interoperability barriers among the communication systems of various PPDR organizations are still present both a national level (among public safety organizations of the same region or nation) and at European level among PPDR organizations from different nations. Interoperability barriers are usually based on historical reasons: communication networks are created by each PPDR organization with a vertical structure to address the specific requirement of the organization. In same cases, interoperability barriers are also due to security reasons. In the effort of securing and protecting the network data, cryptography mechanism and cryptography keys are different in networks based on the same technology. Interoperability barriers are more often operational than technical. Common procedures and organizational schemes during a national disaster may be defined at national level, but not at European level. Cross-border operations are particularly affected by lack of interoperability because of linguistic barriers or because national organizations use different network technologies. A critical issue is the lack of roaming capability, which is available for users of commercial networks (e.g. GSM/UMTS), but it is not available for the PPDR community. As a consequence, a PPDR officer moving from one dedicated PPDR network to another will lose the communication instead of being transferred to the new network.

- **Broadband Connectivity:** Existing or new PPDR applications are driving the need for broadband connectivity to transmit images or video. This need is not the same in the European member states. Some PPDR organizations are comfortable with narrowband data communication like the one provided by the current TETRA networks, while other PPDR organization demand broadband communication to support a number of applications. A description of the PPDR applications is provided in Annex 1. Wireless communications systems based on TETRA and TETRAPOL are currently providing limited data capacity, which may not be enough for many of the listed applications. The implementation of these services however has been inhibited by a lack of suitable radio channels in range 380 MHz to 470 MHz in Europe. Furthermore, the political diversity of Europe is reflected in the variety of spectrum regulations at national level. The new frequency bands for PPDR in Europe should also be harmonized, meaning that the spectrum allocation for PPDR should be the same across the European member states.

- **Underground/Lack of coverage:** PPDR organizations must operate in uncertain conditions and difficult environments. For example, natural or man-made physical structures may obstacle radio propagation and limit the range or QoS of wireless communications. This type of problem is particularly present in underground operations. This is not a specific problem of PPDR communication systems but of commercial systems as well.

- **Degraded or Destroyed infrastructures:** PPDR infrastructure may be destroyed or degraded as a consequence of the crisis. An earthquake, flooding or tsunami can destroy the physical network infrastructure. Even if the network infrastructure is not destroyed, it can be overloaded by the increase of traffic as in the case of the London bombing. While this situation is definitively possible for commercial networks, it is less likely for dedicated PPDR networks like TETRA, which are usually sized for maximum capacity. Dedicated PPDR networks are also designed and deployed with high availability. Logistics facilities and infrastructures may not enough to support the needs of first time responders and volunteers organizations operating in the disaster area.

- **Technological gap with commercial technologies:** Evolving Technologies and standards may cause the existing wireless equipment to become obsolete. The equipment lifecycle in PPDR organizations is less dynamic than commercial environment. A dedicated network and related terminals is usually designed and acquired for a long time (e.g. 10-15 years) in comparison to the commercial domain, where the terminal lifecycle is in the order of 2-3 years. A potential risk is that PPDR communication technology may not follow the technical progress of the commercial domain. First time responders may use networks and terminals built with a technology, which is more reliable but less advanced than commercial systems. PPDR networks must provide specific functionalities, which are often missing in commercial networks. For example: group call where this service offers a circuit-switched walkie-talkie functionality to allow subscribers that have registered to a call group to communicate with all other subscribers in the area who have also subscribed to the group.

## 2.2. "State of Art": current initiatives in Europe and the world

The challenges described in the previous section have been addressed by a number of organizations in Europe and the world in recent years.

Apart from Europe, USA has been most active in this area following the 9/11 terrorist attack in New York and the Katrina disaster. In both cases, the lack of interoperability and broadband connectivity by PPDR communications was painfully evident.

The following programs/initiatives can be a useful reference:

- SAFECOM (http://www.safecomprogram.gov) 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.
  SAFECOM has taken steps on a variety of fronts to improve interoperability. One of the most relevant documents produced by SAFECOM is the Statement of Requirements (SoR) [1], which defines what it will take to achieve full interoperability and provides industry requirements against which to map their product capabilities.

- The recent report by US GAO [2] identifies in continuity of communications, capacity, and interoperability the primary areas of vulnerability in first responder emergency communications in communities across the country. The report focuses on issues related to emergency communications systems used by first responders in the aftermath of catastrophic disasters. Specifically, the report identifies (1) vulnerabilities, if any, to emergency communications systems, (2) federal assistance available or planned to first responders for addressing any vulnerabilities or enhancing emergency communications, and (3) challenges, if any, with federal emergency communications efforts. To identify and examine vulnerabilities, to existing emergency communications systems, the report developed six case studies and subsequent analyses of varying catastrophic disaster scenarios both natural and man-made

- NIST OLES. The Office of Law Enforcement Standards (OLES) helps criminal justice, public safety, emergency responder, and homeland security agencies make informed procurement, deployment, applications, operating, and training decisions, primarily by developing performance standards, measurement tools, operating procedures and equipment guidelines. OLES is part of the Electronics and Electrical Engineering Laboratory (EEEL) of the National Institute of Standards and Technology (NIST).

- The new US National Broadband plan by FCC [10] promotes new approaches to provide broadband communications to public safety. The main proposal, described in the report, is to make available part of the resources of the commercial LTE networks to Public Safety organizations. The idea is to allow the public safety community to realize the benefits of commercial technologies, which will reduce costs and ensure the technological evolution of the networks. In particular, the report advocates an opportunity to enter in flexible spectrum-sharing partnerships with commercial operators. In particular the sharing of the 700 MHz commercial spectrum allocation known as the “D block.”

In Europe, a number of projects and organizations have analyzed the needs and challenge of PPDR organizations in communications including:

- The FP6 SSA NARTUS project established a European platform and roadmap for future public safety communication, in order to facilitate European integration in the area of Public Safety with particular focus on PPDR communications and information systems. The R&D roadmap for future public safety communications is particularly relevant as it analyzes current gaps and identifies key research areas.

- European Security Research and Innovation Forum (ESRIF) Final Report, December 2009, which proposes a European Security Research and Innovation Agenda (ESRIA) over the next 20 years. Reliability and interoperability of PPDR communications is one of the main topics considered in the document. The role of standardization to introduce innovative technologies in the market was highlighted.

- ETSI has a number of committees working in the area of PPDR communications including: Project MESA, which 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, Technical Committee (TC) Emergency Telecommunications (EMTEL), which analyzes the procedures and technologies to establish communications channel between authorities and civilian populations, TC TETRA for the definition of the TETRA standards widely deployed across Europe and TC Reconfigurable Radio Systems (RRS) Working Group 4 for Public Safety, which investigates innovative technologies like Software Defined Radio (SDR) and Cognitive Radio (CR) for PPDR domain.

- The PASR SUPHICE (Secure Unplanned Provisioning of High Integrity Communications across Europe) project which has tried to demonstrate how to set-up and use on-the-fly crypto.

- The PASR project WINTSEC which a precursor on the FP7 EULER project trying to define an EU SDR architecture for the Public Safety domain.

- FP7 EULER project [11], which investigates the use of SDR for PPDR domain as a way to remove the interoperability barriers. The EULER project gathers major players in Europe in the field of wireless systems communication integration and SDR, is supported by a strong group of end-users, and aims to define and actually demonstrate how the benefits of SDR can be leveraged in order to drastically enhance interoperability and fast deployment in case of crisis needed to be jointly resolved.

- FP7 SECRICOM project [12], has the purpose to produce a competitive solution for secure communication and collaboration of emergency responders with advanced functions. SECRICOM address the interoperability barriers, through an IP solution to integrate the many mobile devices already deployed in the Public Safety domain. A full-IP approach is also the essential block to provide a smooth evolution from systems currently developed to systems of new SDR generation.

Others FP7 projects which are dedicated to the support of first responders were DITSEF (Digital and innovative technologies for security and efficiency of first responders operation) and INFRA (Innovative and novel first responders applications).

# 3. Workshop presentations and contributions

The purpose of this section is to describe the contributions of the presenter to the workshop and identify the key messages.

## 3.1. Workshop agenda

The agenda of the workshop is presented in Figure 1 Workshop Agenda:

**Figure 1 Workshop Agenda**

## 3.2. Participants list

| Name and | Company | E-mail address | Country |
|---|---|---|---|

| **Surname** | | | |
|---|---|---|---|
| Emanuele Algieri | Sepura plc | emanuele.algieri@sepura.com | UK |
| Loredana Arienzo | Joint Research Centre - EC | loredana.arienzo@jrc.it | Italy |
| Markus Assel | TÜV Rheinland Group | markus.assel@de.tuv.com | Germany |
| Gianmarco Baldini | Joint Research Centre - EC | gianmarco.baldini@jrc.ec.europa.eu | Italy |
| Peter Baude | TÜV Rheinland Group | peter.baude@de.tuv.com | Germany |
| Mark Bennett | SOCA | mark.bennett@soca.x.gsi.gov.uk | UK |
| Chantal Bonardi | ETSI | Chantal.bonardi@etsi.org | France |
| Hans Borgonjen | Police Netherlands | hans.borgonjen@ito.nl | The Netherlands |
| Egil Bovim | National Centre on Emergency Communication in Health | egil.bovim@kokom.no | Norway |
| Laurent Cabirol | European Commission – DG ENTR | laurent.cabirol@ec.europa.eu | Belgium |
| Michela Cancellaro | Sepura plc | michela.cancellaro@sepura.com | UK |
| Miguel Crisostomo | Telefonica | ut03556@telefonica.es | Spain |
| Franc Dimc | Univ. of Ljubljana, FPP | franc.dimc@fpp.uni-lj.si | Slovenia |
| Ompe Aime Dr.-Ing. Mudimu | Cologne University of Applied Sciences | ompe_aime.mudimu@fh-koeln.de | Germany |
| Chiomento Flavio | French Ministère de l'intérieur | flavio.chiomento@interieur.gouv.fr | France |
| Nils Granath | NearShore | nils.granath@nearhsore.ch | Switzerland |
| Florian Heiser | Siemens | florian.heiser@siemens.com | Switzerland |
| Richard Hlavaty | Defence and Security Industry Association of the Czech Republic | info@aobp.cz | Czech Republic |
| John Holmstrom | Ajeco Oy | john.holmstrom@ajeco.fi | Finland |
| Quema Quemard Jean-Pierre | EADS | jean-pierre.quemard@eads.com | France |
| Jeppe Jepsen | Motorola | tcw029@motorola.com | Belgium |
| Vaclav Jirovsky | Faculty of Transportation Sciences, CTU | jirovsky@fd.cvut.cz | Czech Republic |
| Bernhard Kern | BDBOS | bernhard.kern@bdbos.bund.de | Germany |

| | | | |
|---|---|---|---|
| Klaus Keus | Joint Research Centre - EC | klaus.keus@jrc.ec.europa.eu | Italy |
| Juha Knuuttila | Laurea University of Applied Sciences | juha.knuuttila@laurea.fi | Finland |
| Anna Kotesovcova | Charles University, MFF | kotesovcova@ufal.mff.cuni.cz | Czech Republic |
| Monika Lieberam | BA THW | monika.lieberam@thw.de | Germany |
| Marcello Marzoli | Ministero Interno Dipartimento Vigili del Fuoco | m.marzoli@tiscali.it | Italy |
| Robin Marterer | University of Paderborn / C.I.K. | marterer@cik.upb.de | Germany |
| Julio Martínez Meroño | Ministerio del Interior - Secretaría de Estado | juliomm@mir.es | Spain |
| Ignacio Montiel-Sanchez | European Commission – DG ENTR | Ignacio.Montiel-Sanchez@ec.europa.eu | Belgium |
| Alon Moss | Athena GS3 Security Implementations Ltd. | alonm@athenaiss.com | Israel |
| Patrick Mächler | Siemens Switzerland Ltd. | patrick.maechler@siemens.com | Switzerland |
| Chantal Neyrinck | EUROPOL | neyrinckchantal@hotmail.com | The Netherlands |
| Francesco Pasquali | Selex Communications | francesco.pasquali@selex-comms.com | Italy |
| Jakub Piskorski | Frontex | jakub.piskorski@frontex.europa.eu | Poland |
| Heikki Riippa | Police Technical Centre | heikki.riippa@poliisi.fi | Finland |
| Miranda Saarentaus | Pöyry Finland Oy | miranda.saarentaus@poyry.com | Finland |
| Olivier Sagnes | THALES Communications SA | olivier.sagnes@fr.thalesgroup.com | France |
| Jaakko Saijonmaa | EADS Secure Networks | jaakko.saijonmaa@eads.com | Finland |
| Hermann Seuschek | Siemens | hermann.seuschek@siemens.com | Germany |
| Hanna-Miina Sihvonen | Laurea University of Applied Sciences | hanna-miina.sihvonen@laurea.fi | Finland |
| Andrew Sleigh | Pinoak Ltd | andrew@pinoak.co.uk | UK |
| Norbert | Thales Defence | norbert.Sonnenberg@thalesgroup.com | Germany |

| | | | |
|---|---|---|---|
| Sonnenberg | Deutschland GmbH | | |
| Teemu Tares | Joint Research Centre - EC | teemu.tares@jrc.ec.europa.eu | Italy |
| Daniela Tulone | Joint Research Centre - EC | daniela.tulone@ jrc.ec.europa.eu | Italy |
| Jaakko Tyni | Laurea University of Applied Sciences | jaakko.tyni@laurea.fi | Finland |
| Mikko Utriainen | North Savo ELY Centre/ Tekes | mikko.utriainen@tekes.fi | Finland |
| Ann Vandenbroucke | Inmarsat Global Limited | ann_vandenbroucke@inmarsat.com | UK |
| Johannes Wilde | Fachhochschule Köln | johannes.wilde@moenchengladbach.de | Germany |

## 3.3. Presentations

### 3.3.1. Welcome Speech by JRC (Dr Alois Sieber – EC DG JRC)

Dr Alois Sieber presented the Joint Research Centre (JRC) of the European Commission, the Institute of the Protection of the Citizen (IPSC) and the Unit of Security Technology Assessment (STA), where is Head of Unit. Dr Sieber highlighted the role of PPDR communications and how they must be interoperable, mobile, capable, reliable, secure, user friendly and they have to work flawlessly. He then presented the origins of the interoperability barriers among PPDR organizations and how the barriers do exist at different levels (organizational, laws/regulations, procedures, language and technical).

The main objective of the workshop is to begin a process aiming for interoperable, secure communication systems in crisis situations. This can be achieved with a short term and a mid-term strategy:

- At short term: what processes are needed to secure interoperability of presently available systems? E. g. further standardisation efforts?
- At mid term: what additional research is needed in order to support further features (e. g. larger bandwidth, support of ad-hoc wireless sensor nets, monitoring of supply chain)?

Finally, he highlighted that the findings of this workshop should guide security research in the field of PPDR communications.

### 3.3.2. Introduction by DG ENTR (Laurent Cabirol – EC DG ENTR)

Mr. Cabirol from DG ENTR/H4 has presented the activity on Security Research of the Seventh Framework Programme 2007-2013. He presented the activity of the European Security Research and Innovation Forum (ESRIF), which is a European strategy group in the civil security research domain. Then, Mr Cabirol presented the issues about interoperability in the public safety domain. Despite a number of studies by various projects and organizations, user requirements are still not clearly defined or integrated across Europe. This issue was also confirmed by other speakers during the workshop. One of the reasons is the diversity of PPDR activities and organizations across Europe, which are in the different stages of technological deployment or may have different organizations structures. One other issue is the limited size of the market (and the difficulties to come to a correct estimation) with regards, for instance, to the GSM market. Another one is the co-existence of two different standards (TETRA and TETRAPOL) backed up by competing industrial players. He then presented the different interoperability layers from the SECRICOM project (see Figure 2 from SECRICOM project).

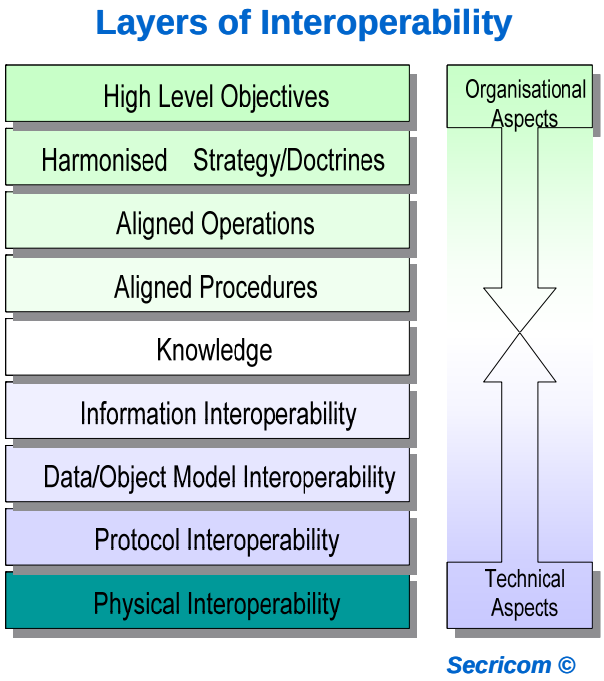


**Figure 2 Interoperability levels from SECRICOM project**

From this presentation, it is clear that Interoperability is not only a technical challenge but also an operational and organizational challenge. Mr Cabirol then presented the main FP7 Security projects, which addresses interoperability:

- EULER http://www.euler-project.eu/ European software defined radio for wireless in joint security operations. How the benefits of SDR can be leveraged to enhance interoperability and fast deployment in case of crisis to be jointly

resolved. Coordinator Thales – From 03.2009 to 02.2011 (36 months). Total value ~ €15.47 M€; Cons. 18 partners / 10 nat.

- SECRICOM http://www.secricom.eu/ Seamless Communication for Crisis Management for EU safety. Solution or mitigation of problems of contemporary crisis communication infrastructures (Tetra, GSM, Citizen Band, IP). Coordinator QinetiQ – From 09.2008 to 04.2012 (44 months). Total value ~ €12.5 M€; Cons. 13 partners / 9 nat.
- INFRA, DITSEF, ESS, COPE
- Projects from DG INFSO (NARTUS, U2010, E3, etc.)

A timeplan is currently defined by DG ENTR to address the PPDR interoperability challenge. Mr Cabirol distinguishes between a short term plan and a long term plan:

- In the short term, the availability of RF spectrum for PPDR and integrated crypto/key management capabilities should the main priorities, even if not purely research issues.
- In the long term, ("beyond TETRA/TETRAPOL") the evolution and the transition from TETRA/TETRAPOL architecture/technologies to new architecture / more promising technologies will be studied, possibly based on the on-going portfolio of FP7 projects rune either by DG ENTR or DG INFSO.

### 3.3.3. Public Safety challenges in the Shengen area (Chantal Neyrinck – EUROPOL)

The presentation was jointly provided by Ms Neyrinck of EUROPOL and Mr Bennet from SOCA.
Ms Neyrinck presented the mission and activity of Europol in the context of Public Safety. The mission of Europol is "Europol's competence shall cover organised crime, terrorism and other forms of serious crime as listed in the Annex affecting two or more Member States in such way as to require a common approach by the Member States owing to the scale, significance and consequences of the offences."
The main capabilities of EUROPOL are its people: top specialists in combating serious crime and terrorism, the representation from all major EU national law enforcement agencies and more than 100 criminal analysts, which makes EUROPOL a centre of EU expertise. The operation department is divided in eight units. The most relevant unit for the workshop is O2 (Centre for Analysis and Knowledge), which coordinates a number of activities including:

- European Criminal Intelligence Model
- Organised crime Threat Assessment
- Social Network Analysis
- Special Tactics- O27
- Terrorism Situation and Trend Report

EUROPOL is currently defining a common platform for experts, to be finalized at the end of 2010 (see Figure 3 from the presentation of Ms Neyrinck):


**Figure 3 EUROPOL Common Platform for Experts**

Mr Bennet of SOCA (Serious Organized Crime Agency) presented the main issues of PPDR interoperability from a user point of view.
We can identify the main issues in the current European situation:

- Technical: TETRA vs TETRAPOL
- Manufacturer against manufacturer
- Roaming of TETRA users from a European member state to another.

The blockages are not only technical but also political. There is a political will at European level to eliminate these blockages ?
One of the most important applications of TETRA/TETRAPOL is to provide Shared Situational Awareness, where location information is provided by GPS (or GNSS in the future). Mr Bennet has presented the SOCA vision on this application.

### 3.3.4.End-user perspective for the interoperability challenges on Public Safety (Heikki Riippa – Police Technical Centre, Police Government of Finland)

Mr Riippa presented a user perspective to the problem of interoperability. In Finland, there is a one national wide tetra network used by the various Finnish public safety organizations (i.e. Police, Fire & Rescue, Frontier Guard, and Customs). As a consequence, there is full domestic interoperability. Countries around Finland have TETRA networks, which may present interoperability issues with the Finnish TETRA network. An overview of the various TETRA systems deployed in Finland and around Finland is presented in Figure 3:

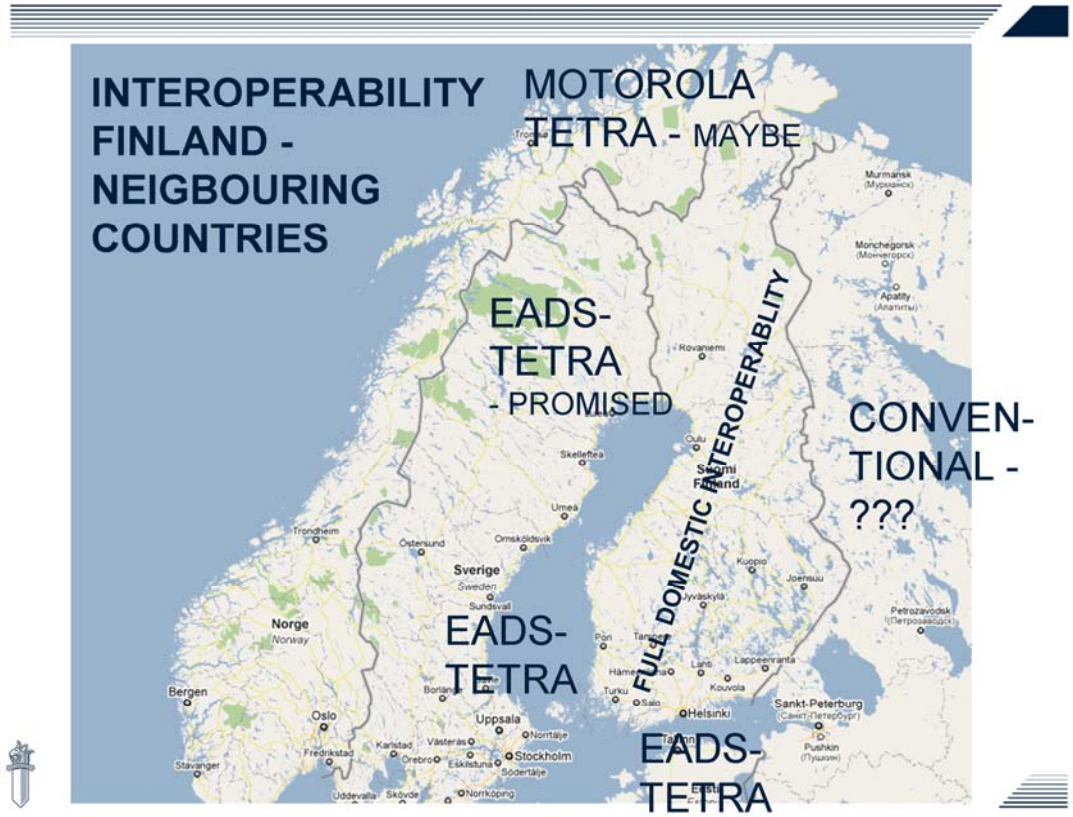


**Figure 4 TETRA deployments around Finland.**

Interoperability solutions are needed for TETRA/TETRA (different vendors), TETRA/TETRAPOL, TETRA/ Conventional PMR and data communications.
Mr Riipa said that data communication is mission critical.
The main effort should be to standardize the interoperability architecture for applications (e.g. command and control) and infrastructure (e.g. interface gateways, mobile unit).
Usability is also a main concern as many solutions are not ergonomic or easy to adapt to existing vehicles or infrastructures.
There is a clear need for ICT standards in public safety.
Mr Riipa provided the following recommendations:

- A joint ISI development for TETRA should be started as FP7 funded project with Roaming as a primary objective.
- Investigate and identify harmonized frequency bands for Public Safety broadband data services.
- There is the need to conduct a feasibility study of TETRA TEDS services to confirm if they are able to address the needs of Public Safety organizations in Europe.
- Standardize and harmonize technologies for PS broadband data network

## 3.3.5. Ten years of SIRDEE: State Digital Radio Communications Emergency System (Julio Martínez Meroño – Ministry of the Interior, Spain)

Mr Merono has presented the digital radiocommunication service for Spanish Safety & Security Forces (SIRDEE). The service (not just a network !) has been deployed in 2000. It is based on TETRAPOL technology, the main user is the Spanish Ministry of Interior and it is operated by Telefonica.
The Spanish security framework is quite complex with:

- State: Ministry of Interior:
  - Guardia Civil (83.000)
  - National Police (66.000)

  Emergency (MoD): 3.000
- Regional Governments
  - 3 Police forces: 23.000
  - Emergency services
- 8.114 Municipalities
  - Police forces: 60.000
  - Emergency services

In this fragmented framework with many users, there are few resources both at RF spectrum level (1.5 MHz), budget and people. As a consequence, cost effectiveness in managing the infrastructure and operations is a strong priority. Sirdee is managed using a Private-Public Partnership where:

- the frequencies are assigned to the Minister of Interior,
- the infrastructure belongs to the contractor,
- new users must be approved by the Minister of Interior,
- the contractor must provide specific levels Quality of Services defined in Service Level Agreements.

Basically, SIRDEE Program Office (part of Minister of Interior) leads and controls the project from an administrative and financial point of view, while the contractor provides communications, complete system & terminal maintenance, and global support. Security aspects are managed by the SIRDEE Program Office.
SIRDEE is a very large infrastructure with 114 centres for operative management, 114 fro tactical management, 1459 base stations, 70,000 terminals, and 14,000 vehicles equipped with Automatic Vehicle Location.
SIRDEE is extremely reliable and secure with >99, 78% Reliability, No security breaches in 10 years of service, end-to-end ciphering. SIRDEE performed very well during emergency crisis (Madrid bombing, Barajas Aircraft Accident) and major events (Spanish royal wedding and Expo 2008).

One interesting information is about use of data communications. The data throughput is limited (3 Kbit/s) but it is still enough as only 3% of the data channel capacity is used. Voice is still the main mission critical application.

In conclusions, SIRDEE is a very successful system. Technical issues are not the main problems, swift & efficient management of resources is essential. The Public Private partnership was quite successful. Shortage of RF spectrum frequencies is still an issue.
The future roadmap is:

- improvement of terminals,
- more coverage and capacity
- incremental development of technologies
- development of new applications
- work on interoperability both at operational and technical level.

### 3.3.6. User requirements and deployment scenarios. (Egil Bovim, National Centre on Emergency Communication in Health, Norway)

Mr Bovim has presented the PPDR issues and challenges from a point of view of emergency health services.
The most common traits of large natural disasters and emergency crisis are serious disruption of expected functionalities, high numbers of casualties and high expectations and pressures from politicians and media.
The use of telecommunications in PPDR is mostly driven by the expectations in the specific scenario. Mr Bovim described some personal experiences: in the tuberculosis epidemic in the Kalahari in the 1980, there were no telecommunications, no interoperability issues but also no support, in 2009/10 pandemic flue, there was an intense pressure for information with any delay and high expectations on treatment. In the malaria outbreak in 1996, the epidemic was well know locally but not at the central headquarters. There were not telecommunication but cheap telemedical devices would be very useful and they would have saved lives.
Telecommunications is basically used by doctors to compensate for the distance. Usability is a major requirement; doctors should not know or worry about the technical details of the equipment. User-friendliness is a major requirement. Other requirements are safety, stability and predictability.
Mr Bovim described in details the services needed for the uplink communications (from local to central) and downlink (from central to local). In uplink, the information transmitted is status of the local site, speech, video, images, and requests for assistance.
In down-link, professional advice from specialist, information on available resources (medicines, transportation) or the environment (weather, access to water resources, planned activities).
Needed commodities are: radio frequency spectrum, user friendly systems, interoperability.
To achieve these commodities, we need to involve all the stakeholders (politicians, professionals, decision makers and highlight the importance of emergency heath service and PPDR in general.
The main problem is that a business cases is difficult to create. How do you value lives ?

## 3.3.7. Interoperability initiatives of the Italian National Fire Corps, (Marcello Marzoli, National Fire Corps – Italy)

Mr Marzoli described the main interoperability issues from a fire-fighters point of view. He identified two main operational contexts for interoperability: interoperability among control centres and in the field.
Interoperability among control centres is particularly complex because of the large number of actors in specific operational contexts (see Figure 3 from the presentation of Mr Marzoli):

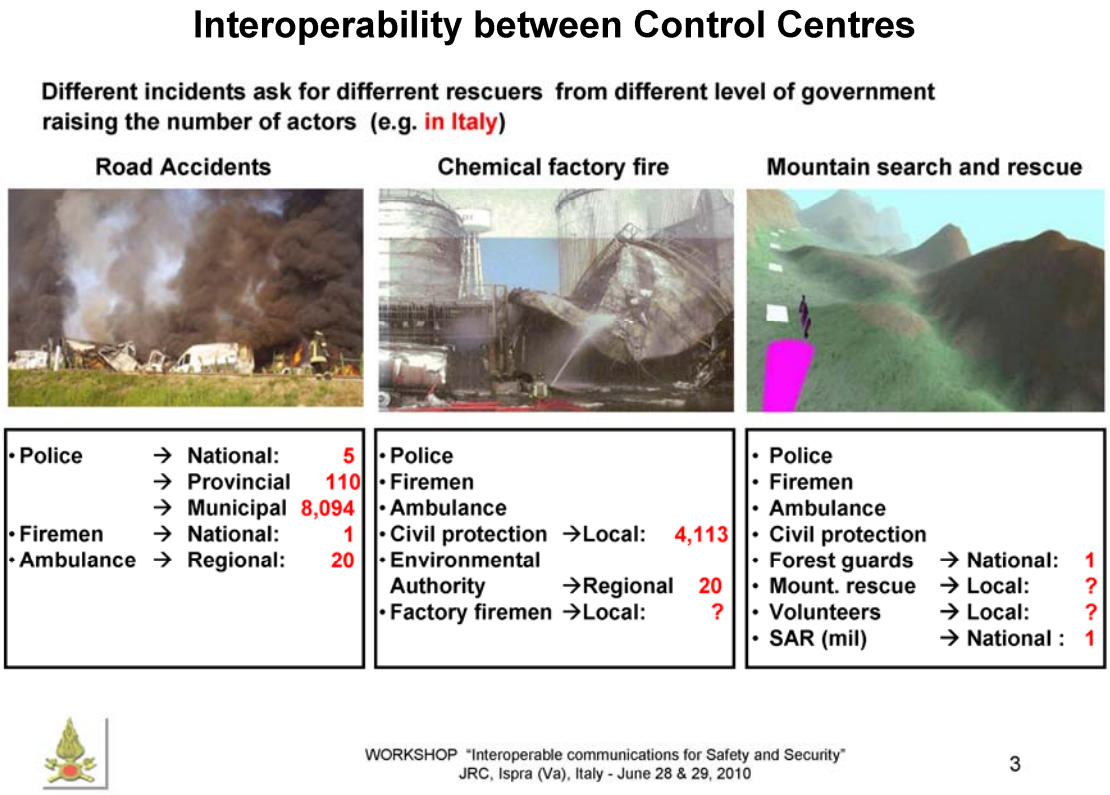


**Figure 5 Command centres involved in emergency crisis**

Currently, each control centre receives information (e.g. voice calls) from citizens or officers in the field to build its common operational picture (COP). Then, the command centre of each organization communicates through voice to integrate the different COPs. The risk is that the resulting COPs are not complete or incorrect. Creating and integrating the COPs is also a long process and control centres may not react fast enough to an emergency crisis.
The most common approach to the issue is to unify all the control centres functions in one only comprehensive control centres. An approach which requires a big deal of political will and risks always excluding some critical service.

An alternative approach is where control centres exchange information through voice, images, video or shared application to facilitate the creation of their COP. This approach requires a close interaction between the control centres and:

- well-established operational procedures,
- wide adoption of open standards and protocols which enable the multilateral exchange of data and facilitate their subsequent aggregation on the receiver side, (e.g. the Common Alerting Protocol (CAP) from OASIS).
- Define bilateral or multilateral agreements to facilitate the exchange of data.
- Adoption of crypto systems responding to widely accepted open standards and protocols so as to facilitate their integration, when needed.

Interoperability can strongly support in field operations within critical infrastructure like metro stations, tunnels, large hospitals. An important element is the capability to determine the indoor location, which cannot be based entirely on GPS or beacon-based systems because radio propagation can be blocked by obstacles. Location aware RFID tags embedded within the emergency devices (e.g. emergency lights, smoke detectors) foreseen by the applicable fire regulations can support mobile or deployable solutions able to provide viable indoor location to the rescuers.
In conclusion the Italian Fire department provided the following recommendations:

- Authoritative researchers and rescuers can choose the best suite of open standards and protocols for a flexible, multilateral Control Centres interoperability.
- Authoritative researchers, rescuers and fire regulation Authorities can choose the best suite of open standards, protocols and formats to design 'location aware' emergency devices.
- Reference implementations can be set up for both issues and made freely available to the stakeholders with the associated documentation.
- Wide dissemination activities and regulatory initiatives can be put in place on both issues to fasten the related standard adoption between the relevant stakeholders.

### 3.3.8. Needs for Mobile Identification: The European MOBIDIG, (Klaus Keus, Joint Research Centre – European Commission)

Mr Keus presented an introduction into the Mobile Identification Interoperability Group (MOBIDIG), which has been established by European national agencies for law enforcement and immigration in 2008 to offer a platform for police and immigration services in the European Union for sharing expert advice and experiences, harmonizing needs and requirements from individual Member States and fostering interoperable solutions for non-stationary applications.
Mobile computing devices are improving rapidly. This has important potential as an enabling technology for policing and immigration, particularly in identifying people, at the border and elsewhere. A smart new generation of mobile computing devices on their own will not solve the problems of identification. How the technology is applied and

used is crucial to its success and it needs to be configured and integrated with existing schemes and systems.

Mobile ID devices may be employed for a variety of applications where stationary booking station type environment is not possible, nor easily attainable. The main scope is dealing with border control and law enforcement applications for the identification and verification of people's identity and for authentication of identity enabling documents through the use of data held in identity enabling documents or held in local and/or remote databases.

The different applications areas and scenarios are numerous. Some common applications for Mobile Id Devices addressed by MOBIDIG are e.g.:

- Authentication of travel and identity documents: using PKI technology to give very high assurance about the integrity of the document, chip and the data it contains and to negotiate approved access (EAC protocol) to sensitive personal data on the chip – fingerprints - for additional assurance that the holder of the document is the correct, authorized holder,
- Fingerprint checks against central biometric systems: to confirm identity and/or to screen against special alert watchlists, e.g. police or immigration,
- Biographic checks against central identity systems: to check what is known about e.g. a named individual (e.g.: is he / she wanted by the police? Does he/ she has a criminal record?) or about a travel / identity document (e.g.: is it lost or stolen?),
- Casework operations: at remote locations requiring more conventional desktop services and access to systems, and possibly enrolment of biometrics,
- Rapid deployment: E.g. to respond to a large number of arrivals at a small, remote port or even somewhere that is not classed as a port,
- Mapping applications: using GPS technology to determine current position and link this to applications.

Various communication systems can be used to support Mobile Id devices and distribute information including TETRA, Satellite, GSM, GPRS and UMTS.
Security requirements (e.g. Confidentiality, Integrity, Availability, Interception, Cloning & Replication,,..) are quite important because data should not be eavesdropped or intercepted. Further topics like Reliability of information, Privacy , Performance (e.g. bandwidth, throughput, response time), new Grid and sensor nets or new sensor technologies (MESH) have to be addressed too.

### 3.3.9. The role of standardization. ETSI and Public Safety Activities. (Chantal Bonardi – ETSI)

Ms Bonardi presented the activities of ETSI in the area of Public Safety.
European Telecommunications Standards Institute (ETSI) is a recognized European standards organization with more than 700 Members from 63 countries from 5 continents.

ETSI works in close collaboration with other international and European organizations including European Conference of Postal and Telecommunication Administrations (CEPT), which is responsible for the spectrum bands allocation across Europe.
Figure 6 shows the links of ETSI with other organizations across Europe and the world.

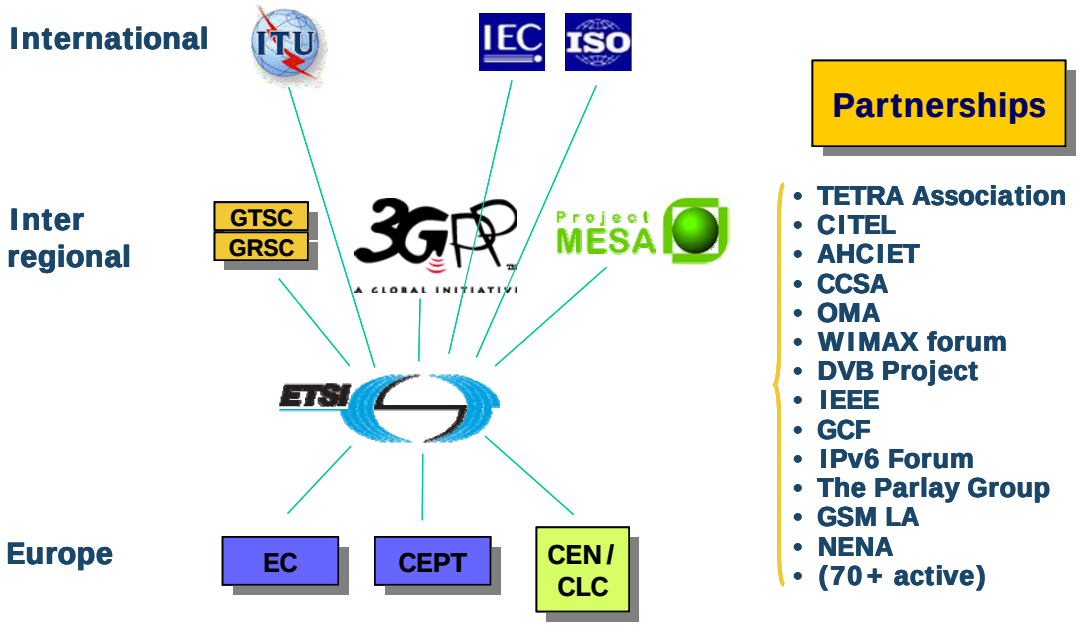


**Figure 6 ETSI relationships with other organizations.**

The ETSI basic principles of standardization are that standards activity should be direct, voluntary, open, based on consensus and public.
Ms Bonardi pointed out that standards are needed to enable growth and innovation. Greater interoperability is an important benefit of standards. It is important that standards are supported and deployed by a critical number of vendors to gain European and (possibly) worldwide acceptance. Standards are needed to reach an economy of scale.

ETSI has been very active in the Public Safety domain for a number of years. A number of technical committees and special committees have been created to support various technical solutions in the Public Safety domain:

- Technical Committee for Terrestrial Trunked Radio (TETRA), which is responsible to define standards for Digital Professional Mobile Radio. TETRA is a outstanding market success. TETRA networks are deployed in Europe and the world (117 countries) and they are used by most of the European Public Safety. The current main challenges for TETRA are additional spectrum requirements for future TETRA systems (which are defined in TR 102 628 to be published shortly) and Inter-System Interface (ISI cross boarder communication).
- Special Committee on Emergency Communications (EMTEL) is focused on defining communications between authorities and civilian population (and vice versa) during an emergency crisis. EMTEL act as a key coordinator in getting European user requirements on Emergency Communications, outside ETSI and

inside ETSI. EMTEL is currently working on requirements for a European Public Warning System (EU-Alert) using the Cell Broadcast Service – TS 102 900.

- Project MESA. International Public Safety Partnership project between ETSI (Europe) and TIA (North America). Produce globally applicable technical specifications for an integrated and innovative digital mobile broadband "System of Systems" for public protection and disaster response sectors. Project MESA has produced important deliverables, which are used as a reference in PPDR studies around of the world. Project MESA is (unfortunately) about to close because there are potentially different goals in North America and in Europe. US has decided to adopt LTE for broadband connectivity for Public Safety, while TETRA is requesting additional bandwidth.
- Mobile cellular, such as GSM/UMTS with eCall. eCall was initiated as working group of the eSafety Forum. eCall aims at issuing an automated call to emergency services, including data to reduce response time of emergency services. Standards developed together with CEN, 3GPP and ETSI.
- Digital Mobile Radio (DMR): ETSI standard defining a direct digital replacement for analogue PMR. DMR has the capability to serve: Consumer and short-range industrial, Professional/Business-Critical applications and Public Safety/Mission-Critical applications. The technology promises improved range, higher data rates, more efficient use of spectrum, and improved battery in comparison to analog Professional Mobile Radio.
- Reconfigurable Radio Systems (RRS) to investigate innovative technical solutions like reconfigurable radio architectures, cognitive radio and flexible spectrum management to the Public Safety domain. TC RRS WG4 on Public Safety has recently published a TR on System Aspects for Public Safety (TR 102 733).
- Satellite communications (SatEC) is tasked to perform standardization in the area of satellite emergency communication in particular involving broadband services, They are currently working on various activities including Multiple Alert Message Encapsulation over Satellite (MAMES), Secunet Infrastructure Network for Civil Securities and Professionals and Emergency Communication Cell over Satellite (ECCS). An important note is that: "A standardisation space mandate will soon be issued and may include disaster management as one of the priority topics"

Finally, Ms Bonardi explained that ETSI is quite committed to support and validate initiatives to improve and ensure the interoperability across various communication systems. ETSI conducts interoperability events and testing events using Tree and Tabular Combined Notation (TTCN) for automatic testing.

### 3.3.10. Spectrum needs and issues for PPDR. (Hans Borgonjen, VTS Police NL)

Mr Borgonjen started his speech with the Council - COMIX Recommendation 10141/09 of the Council of the European Union of Brussels, 20 May 2009, which is a recommendation to improve radio communication between operational units in border

areas. The implementation of the recommendation will require a long term solution for broadband data, which must be based on a harmonised technical solution and a harmonised frequency band at European level. The Council - COMIX recommendation recommended that Electronic Communication Committee (CEPT / ECC) should have the task to study the possibility of obtaining sufficient additional frequency allocation below 1GHz for the development of future law-enforcement and public-safety voice and high-speed data networks.
Mr Borgonjen is the chairman of the Public Cooperation Working Group (PCWG) Radio Expert group Forerunner subgroup, which address the needs for broadband connectivity and tries to identify adequate solutions. PCWG recommendation is that commercial networks are too risky and that harmonized frequencies must be identified. Any proposed solution should consider that a massive investment has already been done in TETRA/TETRAPOL networks in Europe and broadband connectivity should be based on the fact that these technologies will be in use for mission critical voice communication for a long period. The Broadband data solution should therefore not replace the existing networks but should be an addition.

Mr Borgonjen then described the current activity in CEPT as presented by Mr Fatih Mehmet Yurdal of the European Communications Office. PPDR networks are required more and more to provide also broadband connectivity, roaming and interoperability in addition to narrow band and wideband networks. In addition to TETRA there are plans to use wideband and broadband technologies or networks, such as TEDS. TEDS can be used for Wideband. For real Broadband data (e.g. live video) for the time being commercial networks (e.g. 3G) are the only alternative as long as there is no dedicated PPDR Broadband data solution. Frequency bands could be chosen preferably below 1 GHz, because this will decrease the deployment cost of the PS networks.
It is recognized that current spectrum bands allocation is not enough to provide broadband connectivity for PS. The highest bandwidth requirement results from operation categories of “demonstrations and mass events“ and “natural and other major disasters“, not from routine activity. It would be useful to identify the bandwidth requirements for each operational context. There are ongoing studies to determine the needed spectrum.

One key issue is the availability of contiguous and harmonized spectrum. If this is not possible, technological solutions should be identified to adapt a tuning range or a configuration of segmented use of the frequency bands.
A number of solutions have been proposed:

- spectrum sharing between PPDR and commercial networks. In this case, PPDR allows commercial networks to use the shared bands, but PPDR organizations get them back before a Major Event or at the occurrence of a major disaster.
- spectrum sharing between PPDR and military networks. In this solution, the advantage is that authorities for PPDR and military are often the same in European member states. In many countries military is also assisting in PPDR situations, making sharing also a possibility to work together.
- TC TETRA considers that it is necessary to conduct studies on cognitive radio also for broadband PPDR within the 470-790 MHz band.

- Spectrum allocation is preferred below 1 GHz (better below 470 MHz) to reuse the TETRA/TETRAPOL sites.

Commercial networks are not considered an option (at least this CEPT study concludes that for mission critical data communication the use is too risky).

Further work is foreseen for FM38, WG FM and ECC.

FM38 is currently working on identifying the bands for broadband communication in Public Safety. FM38 identified the following bands, which are listed in Figure 7:

- ***225-380 MHz: Limited or no possibility for sharing***
- ***380-385 / 390-395 MHz: Already used for PPDR***
- ***385-390 / 395-399.9 MHz: Part of the tuning range 380-470 MHz for PPDR***
- ***406.1-470 MHz: Part of the tuning range 380-470 MHz for PPDR. Most promising band for additional frequencies for narrow band and wide band PPDR***
- ***470-790 MHz: At the moment very limited or no possibility for PPDR. Possibilities to identify frequencies for PPDR could be reconsidered, if second Digital Dividend (e.g. 698-790 MHz) will be conducted in the future***
- ***790-862 MHz: WG FM has already decided that this band is not an option for PPDR***
- ***862- 870 MHz: Not possible for PPDR***
- ***870-876 / 915-921 MHz: Not suitable for PPDR***
- ***876-915 / 921-960 MHz: Not possible for PPDR***
- ***> 1 GHz: Possibilities to identify spectrum for broadband PPDR could be studied taking into account e.g. the cost differences***

**Figure 7 FM38 study of spectrum bands for PPDR**

FM38 view is that as a first step 2x6 MHz (2x3 MHz for narrow band and 2x3 MHz for wide band PPDR, as proposed in the ETSI SRdoc) additional spectrum should be made available for narrow band (e.g. more capacity and/or coverage in existing networks + extra DMO) and wide band (e.g. TEDS) PPDR throughout Europe. Concerning the broadband PPDR for permanent, day-to-day, wide area use, FM38 is of the opinion that it is yet not possible and it is also too early to identify 2x10 MHz contiguous spectrum for broadband PPDR below 1 GHz.
Further studies are recommended for broadband connectivity. Study is needed to identify the functional needs, related need for spectrum, timing, sharing possibilities etc. This study will be done by FM38 in parallel to the above mentioned work on the 2x2x3 MHz allocation.

## 3.3.11. Secure Border Communications. (Jakub Piskorski, FRONTEX)

Mr Piskorski presented the mission and structure of FRONTEX.

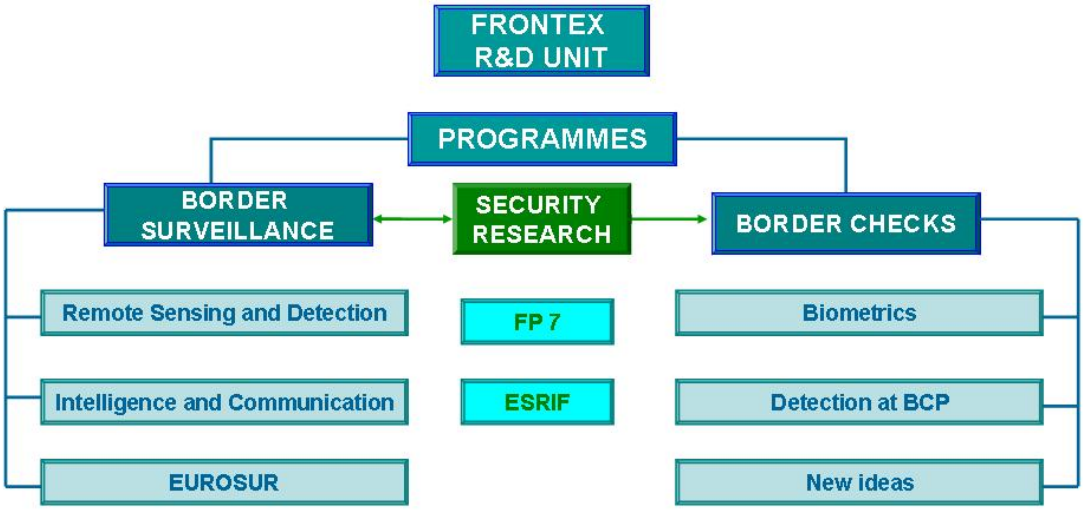


**Figure 8 FRONTEX structure**

The main mission of Frontex is to coordinate the operational cooperation between Member States in the field of border security. The mission of the Research and Development Unit is to follow up on developments in research relevant for the control and surveillance of external borders and disseminate this information to EU Member States and the Commission. The Unit thus acts as a link between the research community and end-users by following and assessing relevant research and disseminating relevant information to end users, but also gathering and summarising the needs of the latter and transmitting them to the those commissioning and performing research. The Unit thus also plays a role in informing the research programmes of the European Union under the FP7 Security Theme and has participated also in policy-development such as the European Security Research and Innovation Forum (ESRIF).Telecommunications is one of the main technologies to support border security operations and thus developments in this area are followed up by Frontex R&D. However, it is important to notice that Frontex is not only focused on technologies, but also on organization and procedures harmonization.

Frontex together with DG JRC and other organizations carried out a study called SEBOCOMM - Secure Border Communications, whose objective was to bring together operational and technical knowledge to help providing European Border Forces with effective, reliable, easy to use communications infrastructure capable of secure, end-to-end delivery of voice and data.
The experience of Frontex is that diverse and competing technologies are currently used: TETRA/TETRAPOL is the most popular, mainly for voice communication, less for data. Interfaces/Gateways are used to interconnect old analogue systems with no encryption. Joint Operations are usually conducted through voice (VHF, GSM), data (email), security (almost none), sensors (radars/cameras), language problems-liaison officers, satellite means are rarely used. TETRA and TETRA networks are predominant. Currently, Frontex is involved in the following activities related to secure communications:

- Definition of User Requirements for a Portable Communication System for direct/group/broadcast calls, bi-directional communication (with common encryption) support for “positioning data”, AIS Positioning System (receiving).
- Manual of procedures for the communication/standardization of vocabulary used in any type of communication carried out in joint operations (based on Communication Manual by IMO).
- Deployment and validation of low-cost gateways (voice & data) testing to interconnect TETRA networks in Estonia and Finland up to 100 users simultaneously (this pilot project was also described in other presentations).

It is worthwhile to mention that Frontex R&D is involved in another large endeavour called EUROSUR, aiming at providing a common technical framework for streamlining the daily cooperation and communication between Member States’ authorities involved in border security. The main objectives of EUROSUR are to: reduce the number of illegal migrants entering EU undetected, reduce the death toll of migrants at sea and increase internal security by preventing cross-border crime. EUROSUR requires the sharing of information of “common interest” excluding personal data, between existing national and European systems. This implies the removal of interoperability and security barriers. In particular, Frontex has been tasked by the European Commission (DG HOME) to carry out a EUROSUR pilot with 6 participating Member States (to be extended), which will be implemented in 2011. The EUROSUR pilot might potentially constitute a playground for testing/exploring the usability and functionality of new wireless portable communication devices, etc.

### 3.3.12. Overview of relevant research overview of relevant research projects and activities on public projects and activities on public safety radio communications. (Ignacio Montiel-Sanchez, DG ENTR H4).

Dr. Ignacio Montiel-Sanchez provided an overview of the relevant research projects and activities financed by the DG ENTR of the European Commission in the field of public safety Radio Communications (PSRC)
These activities are strongly related to the framework defined in European Security Research Advisory Board (ESRAB), which defines security missions:

- Security of citizens
- Security of infrastructure and utilities
- Intelligent surveillance and border security
- Restoring security and safety in case of crisis

and cross cutting activities:

- Security systems integration, interconnectivity and interoperability
- Security and Society
- Security Research coordination and structuring

Dr Montiel-Sanchez explained that research activities in PSRC have a clear role to improve the competitiveness of the European industry in this field.
The Ecorys competitiveness report in 2009 highlighted that the demand is mostly driven by large government agencies (e.g. police forces) with clear national identities and structures. Interoperability is one of the main requirements. There are a limited number of European industry players competing for the high-end segments of the market. USA is still a world leader for commercial and government applications, while Asian manufacturers are attacking the terminals market with low cost equipment.
One of the conclusions of the report is that an adequate standardisation policy and homogenisation of national markets would permit the EU to remain strongly competitive due to its already good position and leadership in mobile and secure communications.

The programming mandate for security standardization is driven by a holistic approach, which considers the operational, procedural and technological aspects. The Security standardization roadmap is defined in the framework of a political context, which includes the European Security Research and Innovation Forum (ESRIF) http://www.esrif.eu, the Study on Competitiveness of the EU Security Industry and the EC Communication Towards an increased contribution from standardisation to innovation in Europe.

In relation to the purpose of this workshop, the standardization mandate has the following specific objectives:

- To enhance secure interoperable communications and data management between the various security control centres, operators, public authorities and first responders.
- To increase the harmonisation of the European security market and reduce fragmentation with the setting of a set of comprehensive European standards.
- To develop common technical specifications concerning interoperability, quality or safety levels, including test methods and certification requirements.
- To provide interoperability and comparability of different solutions, which in turn facilitate and innovation.

A number of projects are currently financed by DG ENTR/REA for Public Safety Communications including:

- **EULER** http://www.euler-project.eu/ European software defined radio for wireless in joint security operations. How the benefits of SDR can be leveraged to enhance interoperability and fast deployment in case of crisis to be jointly resolved. Coordinator Thales – From 03.2009 to 02.2011 (36 months) Total value ~ €15.47 M€; Cons. 18 partners / 10 nat.
- **SECRICOM** http://www.secricom.eu/ Seamless Communication for Crisis Management for EU safety. Solution or mitigation of problems of contemporary crisis communication infrastructures (Tetra, GSM, Citizen Band, IP). SECRICOM tries to address interoperability challenges in Public Safety networks through a common IP-based solution. Coordinator QinetiQ – From 09.2008 to 04.2012 (44 months). Total value ~ €12.5 M€; Cons. 13 partners / 9 nat.

- **INFRA** http://www.infra-fp7.com Research and develop novel technologies for personal digital support systems as part of an integral, secure emergency management system to support First Responders (FR) in crises occurring in Critical Infrastructures (CI) under all circumstances. Coordinator Athena – From 03.2009 to 02.2011 (36 months) Total value ~ €3.8 M€; Cons. 10 partners
- **DITSEF** http://www.ditsef.eu Increase the effectiveness and safety of First Responders by optimal information gathering and sharing, providing self-organising, robust ad-hoc communications where the existing infrastructure may be compromised and investigate and implement novel techniques for 3D positioning. Coordinator SAGEM – From 01.01.2010 to 31.12.2012 (36 months). Total value ~ €4.2 M€; Cons. 10 partners / 6 nat.
- **ISTIMES** http://www.acorde.com/acorde99.html Security systems integration, interconnectivity and interoperability: Optimised situational awareness through intelligent surveillance of interconnected transport or energy infrastructures Coordinator: TeRN - From 01.07.2009 to 30.06.2012 (36 months). Total value 4,34 M€, Cons. 9 partners / 7 nat.

The timeline of the research roadmap is presented in Figure 9**:**
The

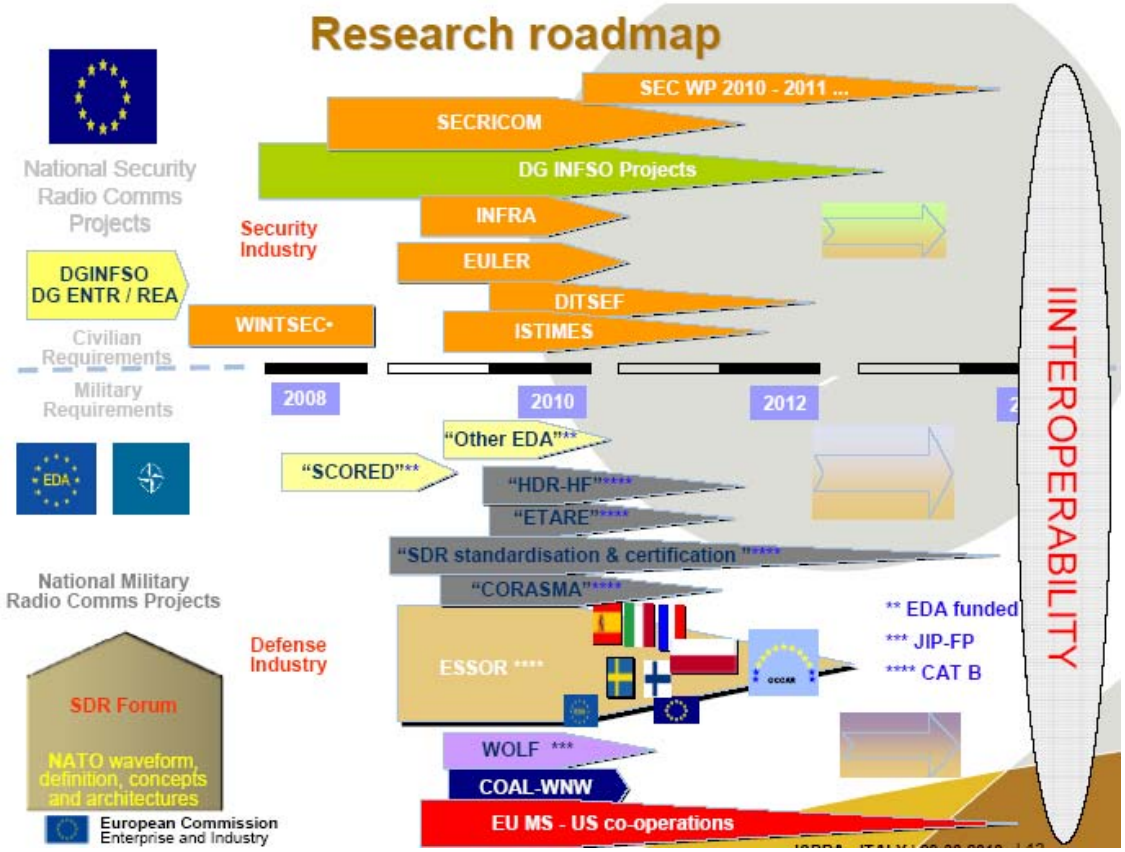


**Figure 9 Timeline for research roadmap**

Future opportunities in the next FP Work program 2011 are for Area 10.5.1 – Secure Communications, Technical solutions for interoperability between first responder

Communication systems and Area 10.5.3 – Interoperability to develop interoperability frameworks, which are focused on the operational level and not only the technological level.
In conclusions, Dr Sanchez provided the following recommendations for a way forward:

- support research & development for interoperability in the higher layers (operational, network)
- investigate synergies between public safety and commercial networks as in the US model, which proposes LTE for Public Safety broadband communication.
- investigate the feasibility of Cognitive Radio to improve spectrum utilization.
- investigate synergies among civil and military markets for the use of Software Defined Radio (SDR).
- In the short tem, support and foster development of existing standards to increase interoperability.

### 3.3.13. Applications for Secure RFID in Public Safety. (Hermann Seuschek Siemens AG, Corporate Technology)

Dr Seuschek presented the use of Radio Frequency Identification (RFID) as an example of short-range communications systems, which can be used for various public safety applications.
Siemens developed a secure RFID device, which can increase the security of the tracking of goods or people for border security or disaster management.
Dr Seuschek described the potential security attacks to a conventional RFID device, which does not have security features. An electrical engineer can easily assemble a fake RFID tag to eavesdrop the communication channel between readers and tags with low cost equipment.
The secure RFID proposed by Siemens has the secure authentication flow described in Figure 10 based on public-key cryptography:

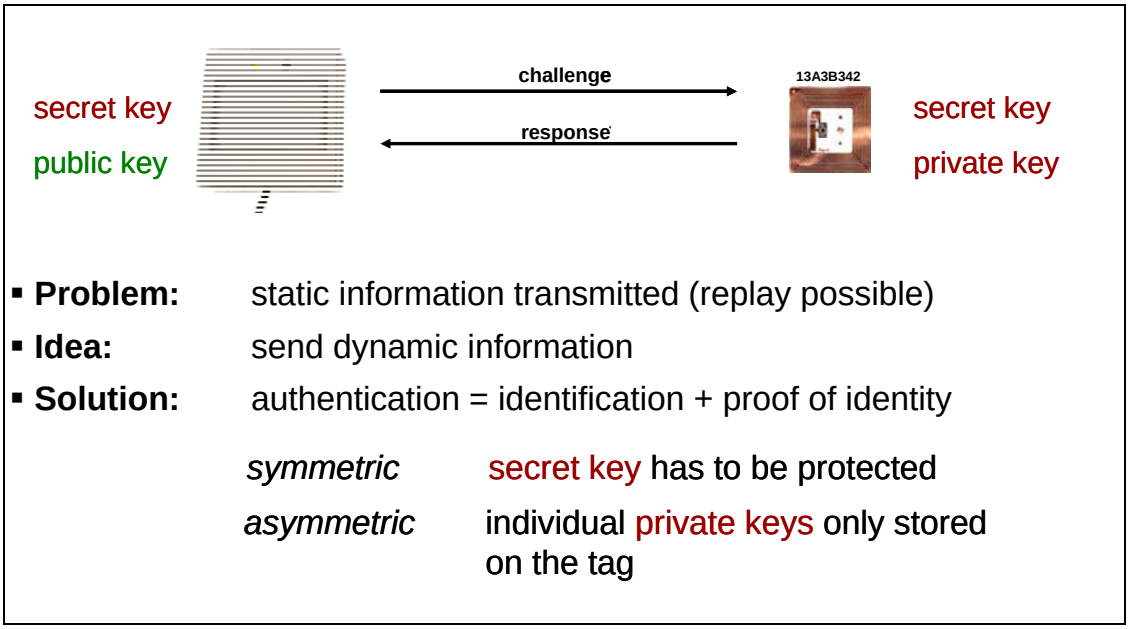


**Figure 10 RFID secure authentication**

The cryptography mechanism is based on Elliptic Curve Cryptography because it is more efficient and adapt to the limited processing and storing capabilities of an RFID.

Secure RFID has a number of Public Safety applications:

- Tracking of goods in Disaster supply chains, where secure RFID can prevent stealing or loss of goods. RFID technology can help to build a secure "virtual infrastructure".
- Transport and warehousing of Hazardous Materials warehousing secured by RFID. RFID tags can store additional information (e.g. inspections of containments, usage of probes, …).
- Securing important documents (e.g. certificate of birth). It is possible to laminate RFID tags with important documents (e.g. birth certificates).

### 3.3.14. Definition of inter-systems interfaces among TETRA and TETRA-TETRAPOL for improved interoperability. (Hans Borgonjen, VTS Police NL)

In his presentation, Mr Hans Borgonjen highlighted the importance of inter-systems interfaces (ISI) among TETRA and TETRA-TETRAPOL for improved interoperability across European borders.

A major issue for TETRA cross border communication is the lack of interoperability capability between the networks. A terminal registered within a national TETRA network can (when programmed with a foreign fleet map and some other pre-arrangements) roam to that network and get limited functionality, but cannot operate with the needed

functionality (because of lack of internetworking interfaces) in that and other TETRA national networks.
A three pilot trial had been in the past among Aachen (Germany) –Liège (Belgium) – Maastricht (The Netherlands) to demonstrate a proof of concept for ISI. Operational research was applied during the operational field trials.
The functional requirements for the TETRA ISI were based on Technical TETRA ISI standard and Interoperability profiles, operational scenarios defined for the three-country pilot scenarios and recommendations from the users (ASTRID, BMI and C2000).
The first phase of the pilot scenario was conducted in 2005.
A number of recommendations were drafted as part of the pilot project:

- Procedures recommendations: fleet map capability with international groups is needed. Dispatching of international forces required specific operational training. Control rooms have to work in close cooperation. Language barriers are also an issue.
- Functionalities recommendations: data capability can be used to address language barriers. Automatic Vehicle Location capability in foreign networks is desired. Status of responders' teams is also recommended.
- Terminal equipment recommendations: the display has to show the active network at any time. The networks should be selectable. Members of the group should be easy to identify. Use of Direction Mode of Operational (e.g. digital 'walkie talkie' mode) is still needed.

The COMIX recommendation (COMIX 421) by the Council of the European Union acknowledges that effective cross-border cooperation requires adequate communication capabilities including interoperable radio communication systems in border areas and between operational services from different Member States.
As a consequence, ISI standards must be defined and the European Commission could provide funding for the development of an ISI prototype.
A discussion among the workshop participants started on this aspect. The main problem is that the funding for this activity cannot come only from research, but it should also come from member states. The research budget of the EC may not be enough to finance ISI and it must also be used for other research activities. Because ISI capabilities are requested by European member states, they should also be involved in the funding decision.
A project proposal submitted at the end of 2009, with the aim to realize an ISI prototype, was not accepted. The focus is now, as a first step, on a much smaller project which should fit into the FP7 program. A project plan with milestones from this new ISI project based on the existing FP7 program was presented by Mr Borgonjen. It is described in:

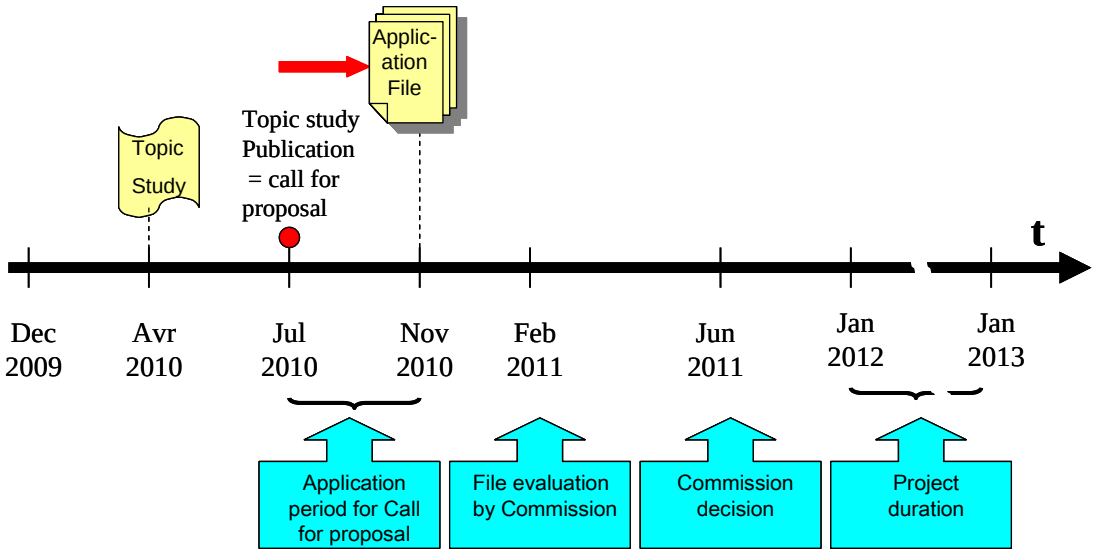


**Figure 11 ISI standardization roadmap**

The recommendation by Mr Borgonjen is that the ISI project could be started as a FP7 proposal in the 2011 call Area 10.5.1 (see 3.3.12). If the proposal is accepted the ISI could be defined for 2013. A further project will be needed to realize the needed prototype.
In the discussion following the presentation, it was pointed out that the deployment/upgrade of the European networks should then be financed by other means, which are not part of the Framework Program (FP).
The biggest challenge is that there are only 5-6 customers across Europe for the ISI. They want ISI but if one of them is the first customer, they do not want to pay for the development of the ISI. The conclusion was that the normal market mechanism does not work in this case, and that the dilemma should be broken by a central funding of the first step (i.e. the development). After that, member states can buy the operational ISI for their network for a 'normal' price. As a consequence, this activity should be financed in some other way or it should be a political decision taken by European member states.

### 3.3.15. Satellite communications applications for Public Safety domain (Ann Vandenbroucke, Inmarsat)

Ms Vandenbroucke described the application of satellite communications to the Public Safety domain and the related regulatory and policy issues.
Inmarsat is providing satellite communication services and solutions in different domains: Maritime, Land and Aeronautical and it has a wide range of customers in military, public safety and commercial markets.
Recently, Inmarsat provided essential communication/remote sensing services in natural disaster/emergency crisis including environment monitoring for the oil slick in Gulf of Mexico, earthquake in Haiti and fighting piracy.

New radio technologies are currently proposed for aeroplanes and maritime transportation to provide high available and effective communications in any condition.

Ms Vandenbroucke described the recent development of and Hybrid satellite – terrestrial (CGC) system in the S-Band (1995-2010/2170-2185 MHz).
CGC has the advantages to allow for smaller, speedier and higher bandwidth terminals and it overcomes "line of sight" issues in metropolitan areas. The bands are also contiguous with UMTS, so terminals should not change the front-end architecture to transmit/receive in CGC and UMTS bands.
S-band satellite services could also be used to for Professional Mobile Radio (PMR). There is wide policy support for S band PMR services including Maritime – 'Blue Book' network requirements, Critical National Infrastructure from UK Government and Public Protection Disaster Relief from CEPT.
S-Band could be used to provide broadband connectivity to Public Safety responders in the field through various solutions:

- Dual use TETRA / S-band terminal, which could provide up to 10 Mbps enabling a richer data service than is possible today with TETRA or in the future with TEDS. Furthermore, dual use TETRA/S-band terminals could have the advantage of augmented coverage in comparison to single TETRA networks, which are based on the terrestrial infrastructure.
- Dual mode S-band / L-band terminal, which can provides up to 500 Mbps broadband service
- Increase the synergy and integration with 4G bands.

Satellite communications provide an important benefit for Public Safety responders as they provide coverage even when the telecommunication infrastructure is destroyed (e.g. for an earthquake).
Figure 12 shows the system architecture for an S-band CGC system.

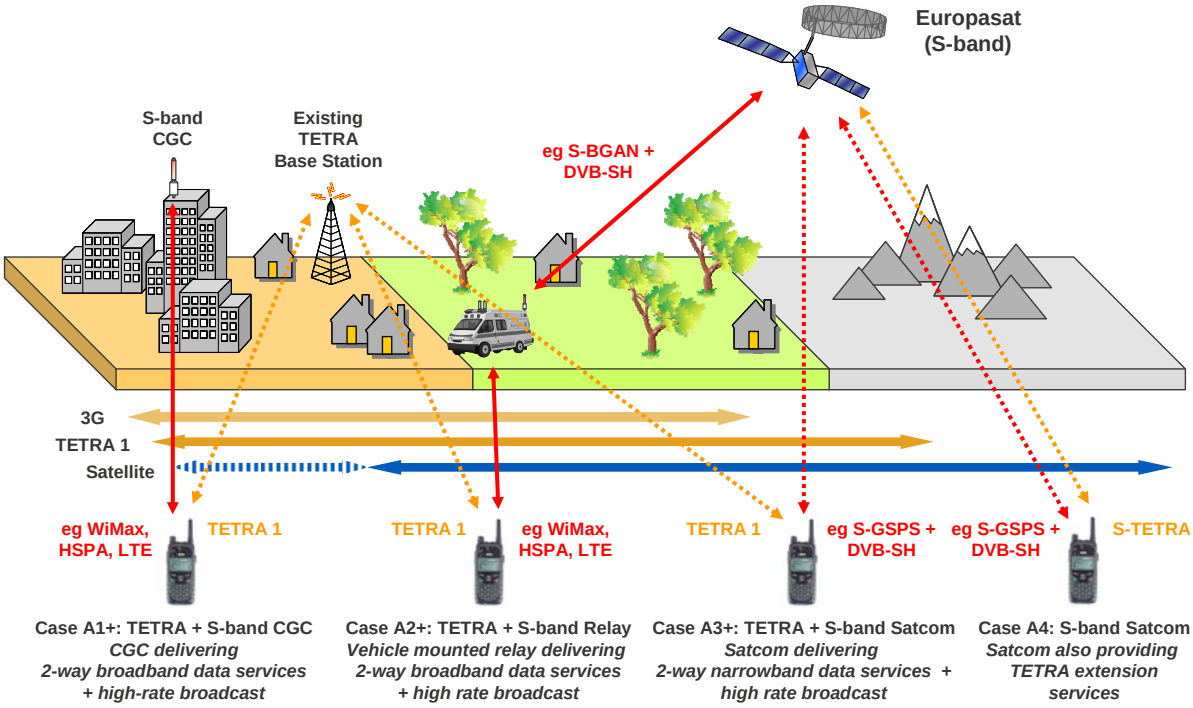


**Figure 12 S-Band CGC system architecture**

The proposed systems can also provide various mechanisms for prioritization and pre-emption.
In conclusion:

- mobile satellite communications are an important technological solution to support public safety organizations during an emergency crisis.
- an hybrid satellite-terrestrial solution could provide higher bandwidth and augmented coverage in comparison to single dedicated networks (e.g. TETRA).
- 80% of Inmarsat traffic is currently data and the future challenges are related to increased data rates. Data communications will be a strong trend for public safety communications in the future.

### 3.3.16. Evolution of Public Safety networks interworking (Francesco Pasquali, Selex-Communications)

Mr Francesco Pasquali described the current situation of Public Safety communications in Europe, where dedicated networks based on TETRA and TETRAPOL are predominant.

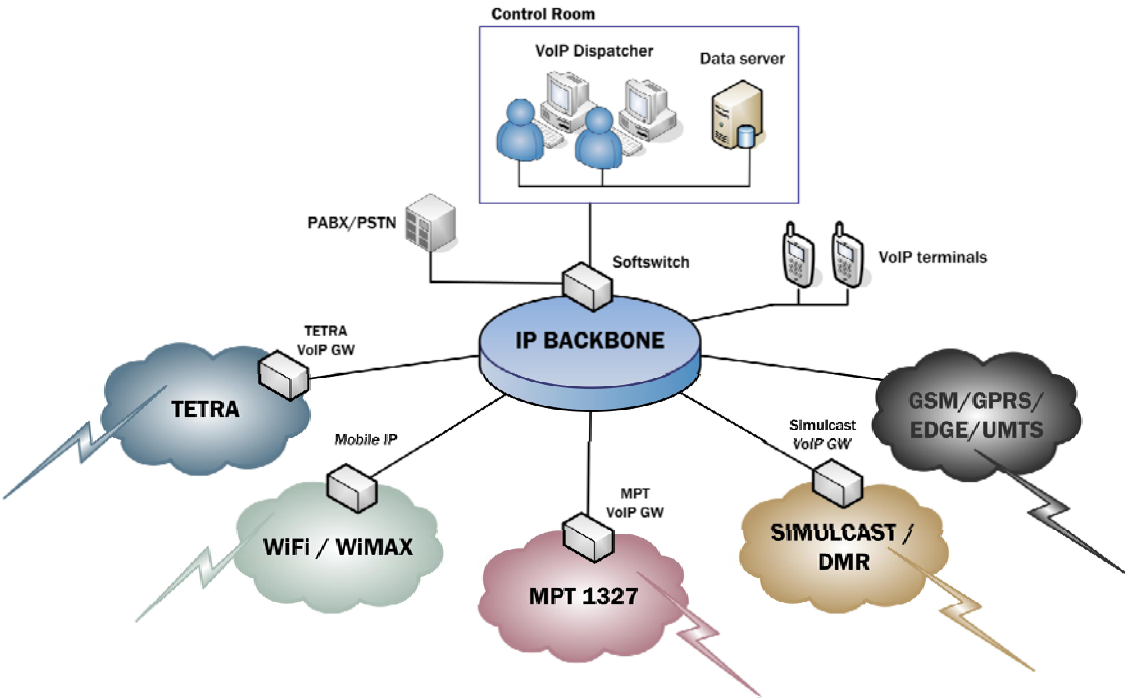


**Figure 13 IP based evolution for TETRA-TETRA ISI and TETRA-TETRAPOL ISI**

Mr Pasquali clearly pointed out that:

- Commercial networks or 3G/4G technologies are unable to fulfill basic PSS user requirements in terms of availability, security, timeliness, RF coverage.
- Dedicated networks are still needed for mission critical voice/data.

Commercial networks can complement dedicated networks for non mission-critical applications.

TETRA recently evolved from circuit switched origin to IP packet switched concepts. The evolution of TETRA towards IP was a market demand, because of its cost effectiveness, easier integration with broadband commercial technologies and possibility to use commercial COTS components. In recent time, the majority of TETRA network suppliers moved from Time-division multiplexing (TDM) to IP based architectures.

Then, Mr Pasquali presented the current activity on the Inter Systems Interfaces (ISI). An ISI standard has already been defined. The activity was started in 1996 and completed in 2000. It is based on a circuit switched approach, Q.SIG and Rose protocols and it is now obsolete.

A new ISI standard must be defined based on IP protocols. The new ISI is still on paper and it will require additional funding for its definition and for the development of proof-of-concepts and prototypes. The new ISI should address not only TETRA-TETRA interoperability but also TETRA-TETRAPOL interoperability.

TETRA-TETRAPOL interoperability is a significant challenge because they are based on different protocols and architectures and no TETRA-TETRAPOL ISI standard is available. Because of such differences, a new ISI based on IP is even more recommended because it would allow bringing both technologies on a common platform and creating synergies with the TETRA-TETRA ISI IP-based. In this case as well, significant funding is needed.

In conclusions:

- TETRA/TETRAPOL are the technologies for Public Safety communication networks now and in the future. They can easily be integrated with other technologies through IP.
- There is a need to modify and innovate the ISI with IP-based evolution.
- TETRA/TETRAPOL can be integrated bringing both on an IP based common ground
- Any TETRA/TETRA and TETRA/TETRAPOL ISI development needs for funding

Discussion:
Questions and discussion was again on the problem of funding of ISI. International cooperation between end-users is still not mature. Public Safety organizations should contact respective member states to highlight the importance of ISI from a political point of view. IP evolution was usually accepted by the audience. Dr Montiel Sanchez proposed ISI working group to discuss the IP evolution with partners of the SECRICOM project. As described in 3.3.12, SECRICOM is addressing the interoperability challenge through IP based solutions.

## 3.3.17. TETRA Intersystem Interconnection (ISI) developments in Europe, (Jaakko Saijonmaa, EADS)

Mr Saijonmaa presented the past and current activity of ISI and the related challenges.
ISI has the purpose to provide two main functionalities: terminal roaming and short message, communication for groups.
The first ISI standard set was completed in ETSI by year 2000. ISI field trials and specifications developed in ´3-country pilot´ by Netherlands, Belgium, Germany and industry was done in 2002-2003. Final report of the trials was delivered in 2003.
The current TETRA ISI standard provides full set of inter-system services: mobility management, individual call, group call, status and short data service, packet data gateways from each network. The most updated version of the TETRA Association performed ISI certification are EADS TETRA rel5.5 and Motorola rel6.1- ISI v2. Furthermore, based on TETRA ISI standard, a static group linking is supported by manufacturers in TETRA TA TIP specification as a way forward to support group calls over ISI.
Beyond the ´3-country pilot´ trial of 2003, EADS is currently (2010) in progress of conducting a Cross-Border-Communications (CBC) trial between Germany and Sweden with MSB and BOSNET. EADS Defence & Security will enable world's first operational cross-border communication between two nationwide operational TETRA networks Germany's BDBOS and Sweden's Rakel networks to trial operational cross-border communications. The trial has the purpose to demonstrate basic roaming and interoperability features between different TETRA networks in two EU member states.
A real operational scenario is planned to be executed to validate the pilot system. It will include roaming of Bosnet users to the Rakel network, group calls and coordination between operational centres. The pilot is based on the current ISI version and includes

additionally control room interoperability, as shown by the DWS for visited network in the figure. The existing EADS TETRA network is ready to support ISI, no additional HW is needed. Any TETRA switch can act as an interconnection element, supporting ISI. Authentication by visited network (using ported encryption keys) vs. by home network through ISI has been resolved.

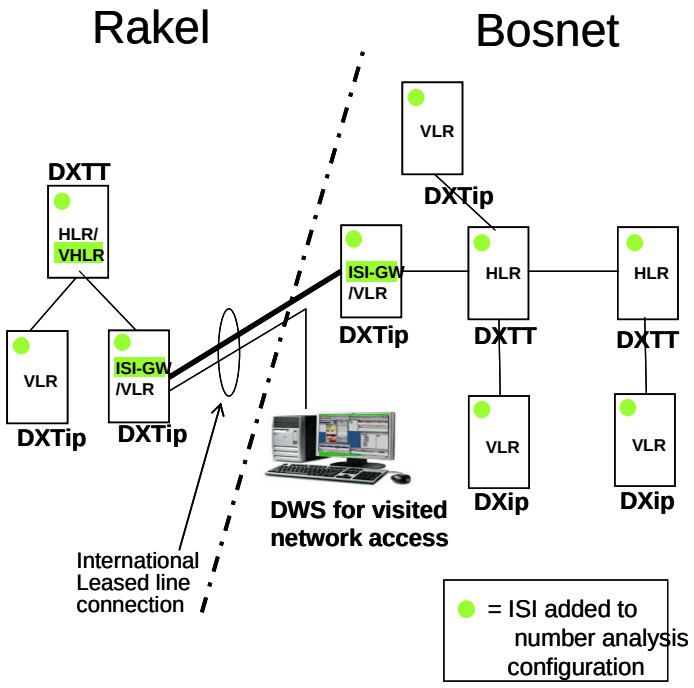


**Figure 14 Functional illustration of interconnection of EADS TETRA networks**

The trial received very positive feedback both from BDBOS and Rakel.
There are still practical ISI challenges to be resolved for interoperability among TETRA networks or different vendors:

- ISI update does not bring much new revenue to TETRA operators, limited international roaming revenues foreseen, if any: financing model needed to proceed
- International interoperation between end-users still at early phase: Funding from end-users is difficult.
- EU/Public financing needed to enable TETRA operator network upgrades to support ISI functionality.

Mr Saijonmaa then discussed the TETRA-TETRAPOL interoperability.
TETRA and TETRAPOL have different architectures and different air interfaces. As a consequence, roaming of TETRA or TETRAPOL terminals into the other network is extremely difficult to implement because:

- architectural differences of TETRA ISI and TETRAPOL ISI require complex change for internetworking between TETRA and TETRAPOL.

- new multi-standard terminals should be developed, which are able to interface both TETRA and TETRAPOL networks. The size of the market is so small, that development cost will not be repaid with the current business case.

One-to-one calls between TETRA and TETRAPOL could be implemented even today, through a simple PABX gateway. Data Gateway can also be used to connect TETRA data network and TETRAPOL data network.
TETRA and TETRAPOL group calls can be implemented, with additional gateway elements, those using TETRA and TETRAPOL ´control room interfaces´. This would provide a static group linking, similar to the user as TETRA ISI group call. Further refinements/developments could be implemented but collaboration with Public Safety users is essential to define main operational needs and prioritize development.

### 3.3.18. Use of Software Defined Radio to support interoperability. (Olivier Sagnes and Bruno Calvet, Thales).

Mr Sagnes presented the EULER project, which is focused on the application of Software Defined Radio for Public Safety and Defence operations.
EULER is an FP7 project started the 1st March 2010 with duration of 36 months. It has a project cost of 15.47 Millions of Euro and the project coordinator is Thales.
The EULER partners include most of the European Public Safety manufacturers and end-users. Thales and EULER partners acknowledge that interoperability is a major issue for Public Safety communications for the following reasons:

- Technical (Inadequate means for first responder communication due to different and incompatible radio systems),
- Technical operational performances ( infrastructures, field conditions … ),
- Non-technical issues (e.g., governance, policies, procedures, and training).

EULER has considered the input from existing and previous projects including Project MESA, APCO 25, TETRA, ETSI RRS, which have already defined requirements and identified trends. Specific waveforms are needed to investigate and test interoperability solutions.
Interoperability is closely related to the different business models and needs for Defence, public safety and commercial domains. Defence and public safety have specific requirements of security, resilience, and Quality of Service. Commercial domain is mostly focused on increasing Average Revenue per Unit. Resilience and Quality of Service are needed and justified only on business considerations.
EULER is also interested to the spectrum sharing model proposed by ETSI RRS, where spectrum can be shared between Public Safety organizations and Defence or Commercial organizations. Standardization is an important element in EULER project.

The approach of EULER is described in Figure 15.

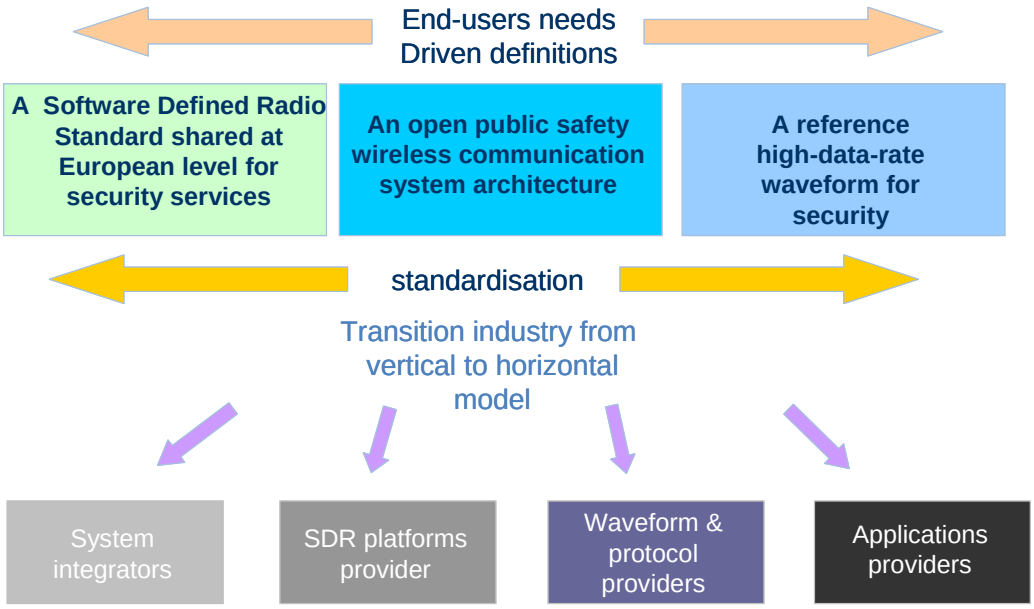


**Figure 15 EULER approach and structure**

From end-user needs and requirements, the project identifies three main elements: the definition of a SDR standard at European level for public safety services (i.e. ESRA), system architecture and a reference waveform for high data rate communication for public safety.
In this approach, EULER will investigate precisely how SDR capabilities can be best integrated in public safety communication system architecture and it will identify a SDR open business model, with separation of roles between SDR platform and SDR waveform providers.
EULER identified portability as a key step for interoperability. Portability is the capability of a waveform to execute on a different HW platform.
The Software Communications Architecture (SCA) is a key element in achieving portability as:

- It enables software elements or modules to be written by different organisations and to be brought together.
- It enables the re-use of some modules, improving interoperability and cost savings.

The high-data rate waveform will be based on 802.16e 2005, with significant tailoring for Public Safety use, which includes support for dynamic spectrum use among networks, additional security features and support for PMR services like call setup, fast communication establishment and group communications. The impact on the spectrum regulatory framework will be considered.

EULER will validate the concepts described so far in a technical demonstrator, which also include a satellite communications waveform. The architecture of the technical demonstrator is described in Figure 16:

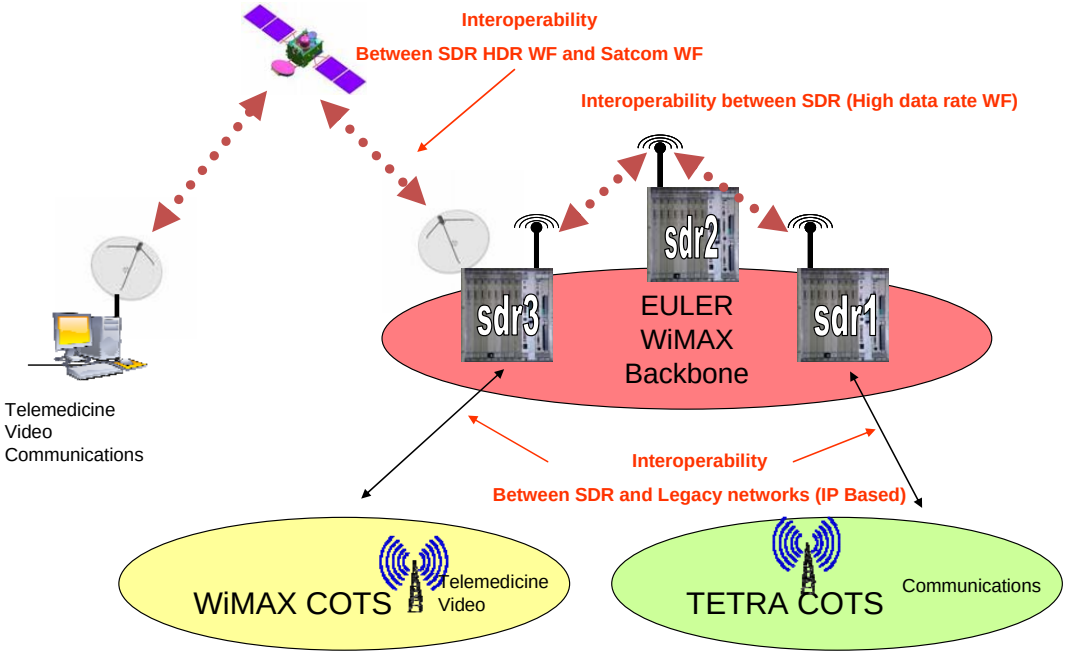


**Figure 16 EULER possible technical demonstration.**

## 3.3.19. DSiP – A solution for Secure Multichannel Communication. (John.Holmstrom, AJECO)

Mr Holmstrom of Ajeco presented the DSiP solution for secure multichannel communication. Ajeco is a small Finnish company (SME) specialized in the field of Security, Industry and Energy utility.
DSiP Is a protocol- and routing-level traffic engineering software solution for intelligently handling data routing, using all kinds of physical media, including IP and non-IP communication with special focus on security and reliability. DSiP can be regarded as a traffic engineering layer above the regular IP-layer.

DSiP allows for:

1. Combining and using telecommunication methods in parallel so that multiple connections appear like a single reliable connection. DSiP can route data over both IP- and non-IP connections.
2. DSiP is independent from operators. It allows the user to shop and combine telecommunication from any operator.
3. DSiP contains protocol translation methods making equipment, systems and software compatible.
4. DSiP implements security mechanisms and reduces risk for DOS attacks & virus-infusion.

DSiP can be used for various applications, which require secure and reliable communications including telemetry and sensors surveillance.

The main concept of DSiP is presented in Figure 17, where the application does need to know on which connect it is sending data as the DSiP system will take care of merging the IP address before the control room used by the Public Safety organization.

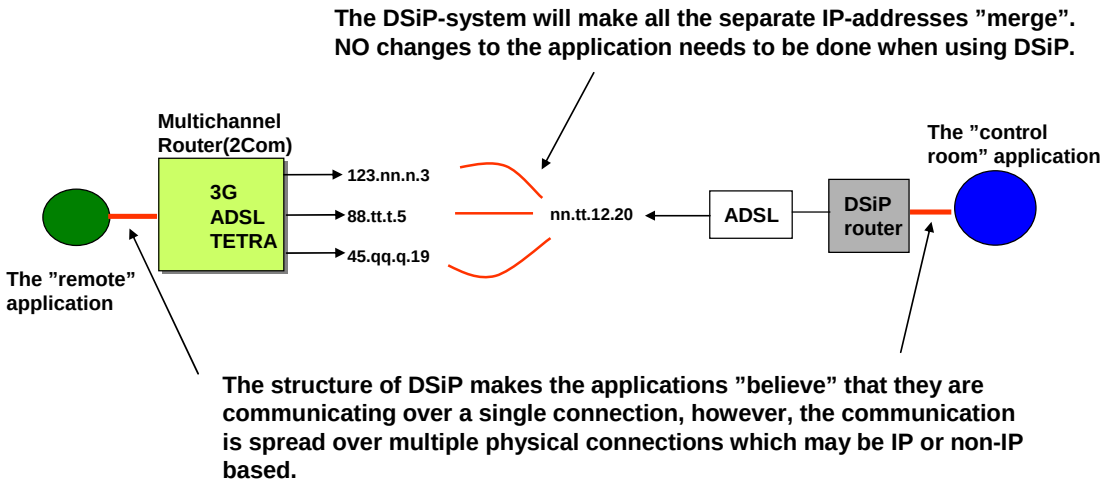


**Figure 17 DSiP concept.**

DSiP has various features and benefits including redundancy, bandwidth control, scalability, complete independency of physical communication methods and security functionalities (e.g. data integrity and authentication).
DSiP can also act as a bridge providing translation capability among equipment and systems of different vendors.
DSiP was used for various projects including the Fingrid main power transmission grid control, coastal surveillance for Finnish Frontier Guard, the FP7 project I2C for "Coastal Surveillance, Sensors & Secure Communication" and the FP7 project PERSEUS for the Protection of European seas and borders through the intelligent use of surveillance.

### 3.3.20. Adaptable sensor networks to support a wide range of sensors. (Vaclav Jirovsky, Czech Technical University, Prague).

Professor Jirovský of the University of Prague presented his research activity on adaptable sensor networks to support a wide range of sensors, which can be used for Public Safety applications in border security and surveillance.

Sensor networks have specific features in comparison to ad-hoc networks:

- Self-organizing capabilities
- Short-range broadcast communication and multihop routing
- Dense deployment and cooperative effort of sensor nodes
- Frequently changing topology due to fading and node failures
- Limitations in energy, transmit power, memory, and computing power

Sensor networks can be dynamic and static. A dynamic sensor network must have capabilities of ad hoc reconfiguration, short transactions and fast reconfiguration algorithms. In a static sensor network, configuration is a controlled process; transactions with large data packets are possible.

Sensor network have a variety of applications including earthquake early warning, snow avalanche early warning, border security application and forest fire detection.
Each of the applications has specific challenges and constraints. For example: in the monitoring system for forest fire detection, information fusion is an essential functionality. Information fusion can be centralized, autonomous or hybrid.

The hybrid solution is presented in Figure 18:

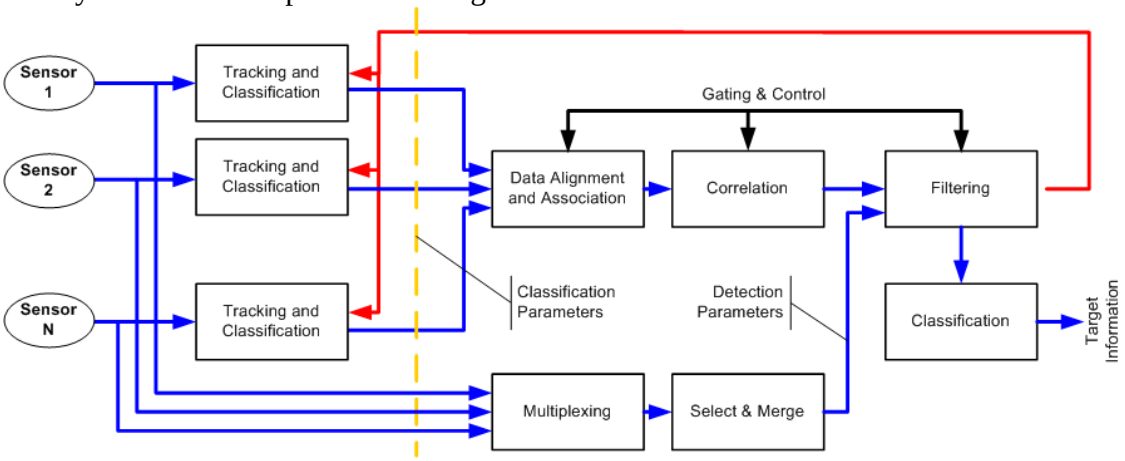


**Figure 18 Hybrid solution for information fusion in Sensor Networks**

Sensor Networks could use communication systems already assigned to Public Safety organizations like TETRA and TETRAPOL. These communication systems provide the level of security and resilience needed by sensor networks.

## 3.3.21. Future Broadband Networks and Terminals. (Jeppe Jeppsen, Motorola).

Mr Jeppsen started the presentation by highlighting the huge difference between spectrum allocation in Europe and USA. Europe has around 10 MHz of spectrum allocated to Public Safety in comparison to USA with 97.2 MHz of spectrum.
TETRA technology has a rich set of features, which are essential for Public Safety organizations but they are not present in other wireless communication technologies. This is another reason why TETRA is the preferred choice for Public Safety organizations.
As mentioned previously, Interoperability spans various layers from organizational aspects, procedures aspects to technological aspects.
While TETRA provides essential capabilities to Public Safety organizations, a lot of features/capabilities could still be developed including better integration among the command centres, multimedia delivery to devices with different capabilities, seamless

operation across bearers from TEDS to broadband and introducing enterprise efficiencies to public safety workflows.
Public Safety could follow the evolution of commercial communication systems, which from simple terminals reached the wide variety of customer centric applications & services.
TETRA TEDS is a major step in this evolution.
Mr Jeppsen described the differences in terms of coverage among TETRA TEDS and commercial systems like LTE, WiMAX and MESH networks. TETRA could provide coverage of 25 Km radius in rural environment and 3 Km radius in urban environment.
TETRA TEDS could also provide a rich set of feature and services in an integrated framework, whose main elements are described in Figure 19:

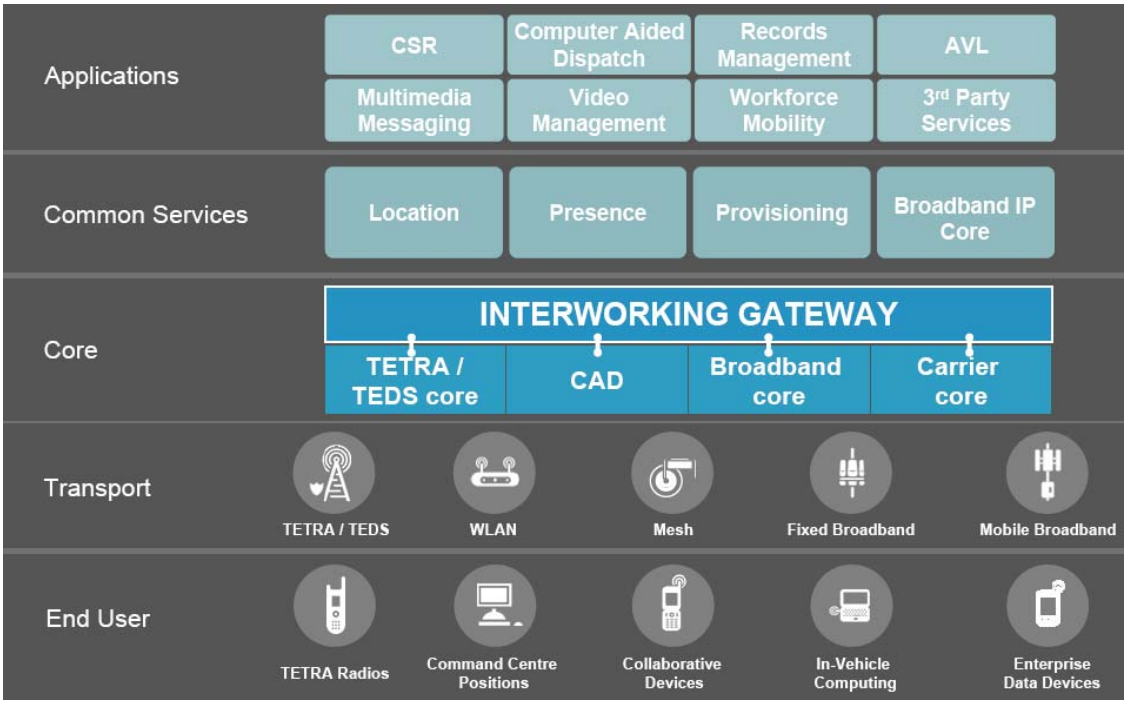


**Figure 19 TETRA TEDS architecture**

Mr Jeppsen described realistic scenarios where TETRA TEDS and related services could be used. For example, during a pursuit on foot, the terminals participating in a group call could send images of the fleeing suspect or automatically collect and distribute data and records associated to a specific position.
TETRA TEDS devices are already appearing on the market, which can be used by customers for increased data usage.
Then, Mr Jeppsen pointed out to the differences between commercial systems and dedicated TETRA networks. The commercial systems do not have the resilience, capacity and security of TETRA systems; because economy dictates their capabilities and they are not designed for this reason.

In summary:

- Mission Critical (MC) voice will stay on TETRA for the next 5-10 years.
- MC wideband data will be provided only by TEDS.
- Public data services could be used but their availability cannot be guaranteed. This has a major impact for operational procedures.
- MC broadband requires additional spectrum.
- Future Public Safety devices must be multi-band standards to address interoperability and to be able to interface to various communication systems.

### 3.3.22. PMR Gateway System & Concepts. (Heiser Florian, Siemens).

Mr Florian described how Siemens is currently active in many projects in the area of Public Safety. One of the projects is Polycom: Swiss secure radio network for authorities and organizations with security functions based on TETRAPOL technology, which will be completely rollout in 2012. Polycom is a large network with 50 control centres, 750 base stations and 40000 terminals. A major issue is the lack of interoperability between TETRA and TETRAPOL.
The status of the ISI in digital PMR is that there is no current TETRAPOL ISI, TETRA ISI has been defined and tested in pilot project but it is old and they are some issues (e.g. QSIG problems). APCO P25 ISSI does exist and it has been tested.
Siemens has developed a PMR gateway, which also addresses security aspects.
The description of the deployment of the PMR gateway is provided in Figure 20:

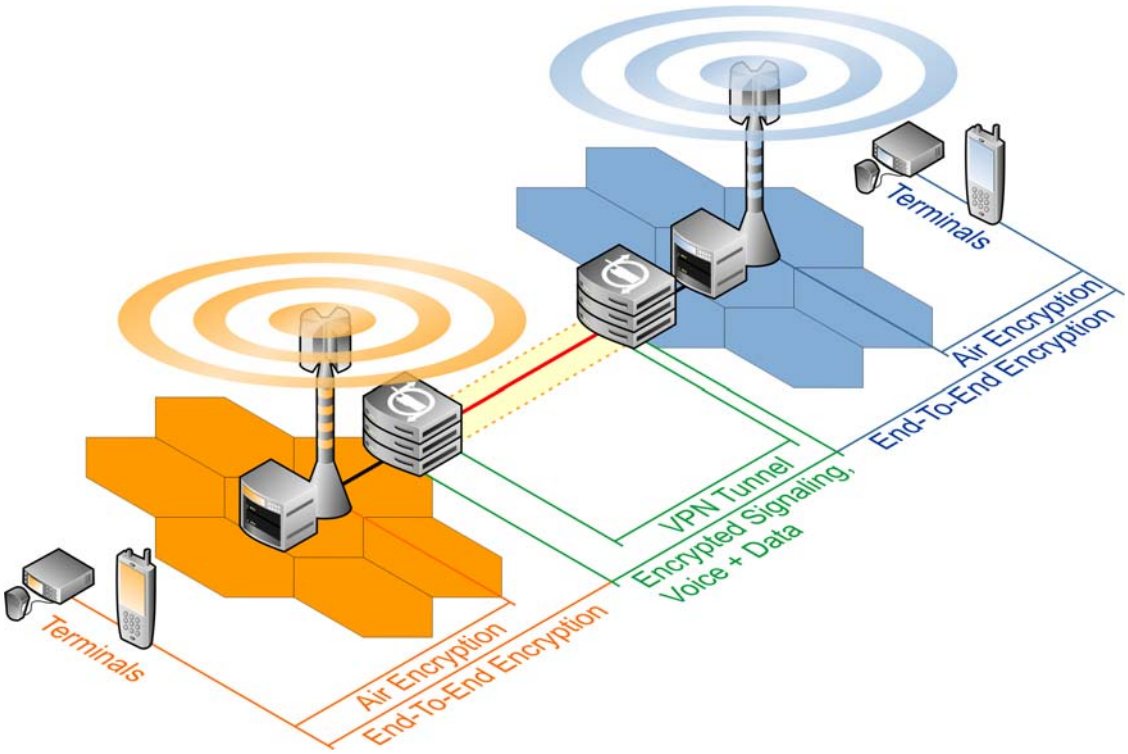


**Figure 20 SIEMENS PMR gateway**

## 3.3.23. Emergency networks. Other Broadband alternatives. (Miguel Crisostomo, Telefonica).

Mr Crisostomo presented the potential path for the evolution of Public Safety communications in Europe. Most of Europe has upgraded the Emergency networks to digital solutions but they lack broadband connectivity. In the commercial domain, a number of broadband services and applications are offered to users. Public Safety should follow a similar path.

The communications of Public Safety officers and control rooms are now predominately **voice** based with limited data support for messaging and database query maps.

In the next generation of public safety communications, the control rooms will require broadband applications to exchange images, video, data from sensors (e.g. finger prints, plates, body sensors), mapping (locations of resources) among them and with the officers in the field.

A huge number of applications are being developed in the commercial domain. Some of them could be used to support Public Safety officers. The adaptation of some applications to the emergency environment will be implemented selecting the most appropriate services, and adjusting their characteristic to mission critical situation, where and effective and quick response is essential. Voice will be the most important application in mission critical situations, but some new applications will be added to the normal operations when they demonstrate their effectiveness and convenience. There will be also non mission critical applications aiding the normal organizations work, not requiring mission critical characteristics, but providing information for the operational databases.

Main applications for Public Safety may be:

- Images and Video applications to transmit relevant images to the control room like the license plate of a suspected car, fingerprints image of a potential criminal, video surveillance and so on.
- Applications for location and guiding (AVL). Controls room should have the position of all the officers in the field like vehicles and people. AVL does already exist today but some features are still missing. In the future, it should be possible to send AVL to the officers themselves or integrate the AVLs of various organizations.
- Sensors on the environment (e.g. forest fires) or to monitor the health conditions of public safety officers (e.g. fire-fighters).

A number of broadband communications technologies can support these applications. We can have three different potential evolution paths (see also section 6):

- Broadband evolution of private and dedicated networks (e.g. beyond TETRA TEDS). Maintain the current voice radio communications system, while the next generation system is deployed, and swap all the services when all the desired characteristics are available in the Broadband network installed.
- Use of commercial networks. Maintain the current Voice Radio communications system, using in parallel commercial services (3G - > LTE), and swap all the services when all the desired characteristics are available in the Commercial network available

- Mixed Private – Commercial Network (e.g. LTE). Maintain the current Voice Radio communications system, using in parallel commercial services (3G - > LTE), maintaining both systems working, each one optimized for their assigned applications set.

The “broadband” evolution of Public Safety is intensely discussed both in USA and Europe:
US has proposed an interesting approach as part of the recent National Broadband Plan:

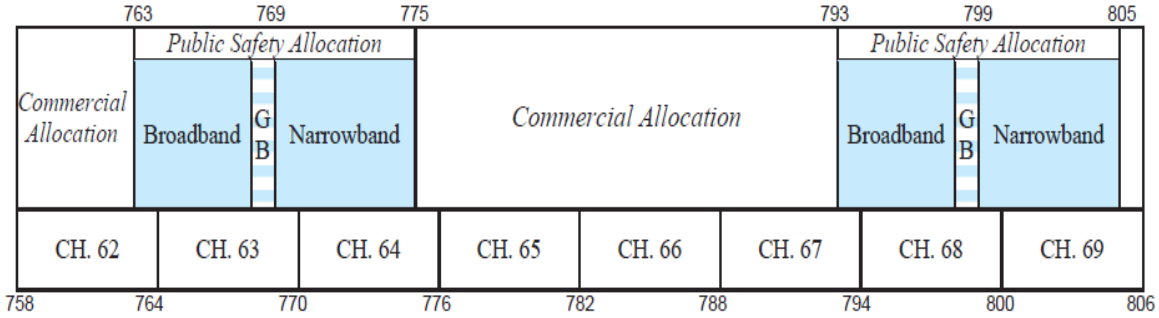


**Figure 21 National Broadband Plan**

In the new National Broadband Plan, there were 2x5 MHz free in the adjacent band (Block D) to be auctioned as a public/private license (commercial exploitation with emergency services priority). These frequency bands are supposed to be used by LTE technology.

FCC is going to auction Blok D in 2011, but it is ensured that all Emergency fleets will access with priority to the services in the whole 700 MHz band. To control these access it has been built a specific organism **ERIC** (Emergency Response Interoperability Centre).

Therefore FCC, in its National Broadband Plan, ensures:

- PPDR broadband communications will be interoperable in all country and jurisdictions.
- National Coverage.
- A reserved capacity, redundancy and liability using priority and roaming over all commercial broadband networks.
- PPDR services will be technologically updated, including terminals at consume market prices.

There is an intense debate on this proposal. Some public safety organizations have already selected LTE as interoperable technology, coinciding with Verizon and ATT LTE deployments in this band.
Other public safety organizations don't want Block D to be auctioned, bur assigned directly to emergency communications use.

In Europe, Digital Dividend is being implemented from 2008 ending the process in 2012. There are a lot of activities to find at least 2x10 MHz band below 1 GHz for PPDR use,

but this is quite difficult because the bands should be “harmonized” across European member states.
Finally, Mr Crisostomo presented the potential broadband communications technologies, which includes Long Term Evolution (LTE), WiMAX and iBurst.

# 4. Panel Sessions

## 4.1. User Perspectives

The panel session on the User Perspectives concluded the first part of the workshop dedicated to Public Safety end-users needs and requirements.

The following conclusions were drawn from this first part of the workshop:

1. Interoperability is perceived by all the users as major issues but there are not only technological implications but also operational and political aspects. In some cases, public safety organizations do not want to interoperate to avoid disclosure or access to sensitive data from external organizations. In this case, a reliable security infrastructure must be created.

2. The requirements for interoperability and broadband connectivity are still not clearly identified in Europe even if many studies have been conducted by different organizations (see references [8], [11]). One of the reasons is the highly fragmented context of European organizations. There are many different organizations with different roles and functions and specific requirements depending on the geographical or geopolitical context. During the workshop, it has been proposed that a European Union entity, which has a close contact with Public Safety users organizations, could draft and maintain the set of requirements, by assembling and streamlining existing contributions. An important task would also be to coordinate the existing Public Safety end-users group existing in Europe. The European Union entity responsible for this activity could be EUROPOL, DG JRC or FRONTEX.

3. The need for broadband communications is not the same across different European member states. In same member states, voice is still the predominant critical mission service; broadband data is not considered essential. In other member states, many PPDR applications have already been created and deployed based on broadband or at least wideband communications.

4. For broadband communications, there is a difference between uplink and downlink connections, which is not clearly specified in many reports. The identification of the applications mostly based on uplink or downlink communications can help to prioritize and define the needs for broadband connectivity.

5. Many participants highlighted the need to promote the case for interoperability and broadband communication, by providing studies, which quantify the

beneficial impact of improved interoperability and broadband connectivity. This can be achieved thorough modelling simulations or through field operational scenarios/pilot projects like the one conducted in 2003 and described in 3.3.10. DG JRC and other partners could provide such quantitative analysis through modelling.

6. One of the biggest challenge for operation interoperability is the lack of a common lexicon of terms and definitions at national level (among different public safety organizations) and at European level. This challenge has been addressed by the OASIS project through the Tactical Situation Object (TSO) and the following CEN workshop 'Information System for Disaster and Emergency Management'. (http://www.tacticalsituationobject.org/index.html). The TSO is complemented by the CAP (Common Alerting Protocol). The CAP still needs to be tailored and maintained to be used for exchange of information among control centres at European level.

7. Some functionalities are more important than others. It is important to identify which functionalities should be made interoperable first. For example: voice group call or messaging could be more important than videoconferencing.

8. The consensus among users is that there will be no major changes to the current public safety network infrastructures (e.g. TETRA). There will be incremental change and the development of new applications. This is also due to the cost of creating and maintaining such large dedicated network infrastructures. Efficient management is one of the main priorities.

9. Usability of the terminals and equipment is quite important. Precious time can be lost if the first time responder must understand how the terminal works. The feedback is that current systems are not totally usable. Related to usability is also overload of information. Public Safety responders need the right information at the right time, they cannot afford to waste time going through unneeded data or communications. Research in Human-Computer interfaces could help.

## 4.2. Critical gaps in regulation, standardization and research

In the panel discussion, the following observations were made:

1. The largest regulation gap is the allocation of spectrum bands to Public Safety at European level. As described in 3.3.21, allocation to PS spectrum bands in Europe is quite lower than the USA. To limit the deployment cost, the bands should be allocated below 1 GHz, preferable below 500 MHz, so that TETRA base stations and terminals should not be replaced.
2. Even if Public Safety is quite important for the protection and security of the citizen, the market size is relatively small in comparison to the commercial

domain. As a consequence, the investments in technology are smaller and the progress in standards is slower than the commercial domain.

3. Standardization activity in Public Safety is well represented in ETSI. This is strong point in Europe. TETRA is a clear success not only in Europe but also in the rest of the world.

4. Research and standardization are important drivers to enhance the competitiveness of EU industry. There should be political support at European level to drive standardization in this sector and support European industries especially SME.

5. There is the need to define a formal process at European level for proposing, commenting upon and agreeing on the evolution of standards. End-users should be more involved in the standardization process to drive identification of needs and requirements.

6. There is still a wide communication gap between end-users and research in the Public Safety area. FP7 projects or industries can close this gap. European Union organizations can also have an active role in translating end-users needs to research activities.

7. Human-machine interfaces are an area where research and standardization could bring strong benefits by improving the adoption of new technologies and improving the operational capability of first time responders.

8. There is a need for a closer integration between commercial networks and public safety networks, with the consideration that commercial networks are usually not designed for the requirements of reliability, availability and security needed in the Public Safety domain.

9. There is a need for application of operational research to the Public Safety domain: the analysis and improvement of operational procedures and organizational structures. Operational research could provide frameworks and decision tools, which could be embedded in the technological elements like applications, gateways and terminals.

## 4.3. Discussion on the technical enablers

A number of innovative technologies were presented during the workshop by some of most important companies in Europe. Technologies can be used to support a number of operational capabilities including improved cooperation among responders, collection of data from sensors, creation and distribution of the Common Operational Picture (COP) and tracking and tracing of goods and people. Most of the presented technologies addressed the challenges of interoperability and broadband connectivity.

In the panel discussion, the following observations were made:

1. The choice of the technological solutions is based on a number of constraints, which includes: cost of the deployment and upgrading to the new technology, usability, security, reliability, availability and easy integration in existing procedural and operational frameworks. Cost of deployment and integration is usually the main constraint as Public Safety organizations have already done significant investments in dedicated network infrastructure and new solutions should be an evolution of that infrastructure rather than a replacement.

2. SDR and CR have been considered by some representatives in the workshop too innovative for short term deployment in the Public Safety domain. Some representatives at the workshop claimed that SDR and CR may still need 5-7 years for practical deployment. Nevertheless, it is important to investigate these technologies and promote the standardization effort as the standardization may take at least 2-3 years.

3. Gateways were unanimously considered a good term solution to address the interoperability problem. The challenge is to identify which functionalities the gateways should provide. Feedback from users would be quite useful to prioritize development of gateways features.

4. The experience from the SECRICOM project and representatives of the workshop pointed out that future networking technologies should be based on IP.

5. While dedicated networks will provide the main connectivity resources to Public Safety officers, specific technological solutions like Satellite communications can provide the needed connectivity where the dedicated networks do not provide coverage, they are destroyed or overloaded.

# 5. Key observations from the workshop

The following key observations were recorded during the workshop:

- Interoperability in Public Safety requires a complex mix of standards, profiles, procedures, system management and policy. During the workshop it has been repeated that interoperability is not only a technical issue but it is also an organizational and political issues. There may be technical solutions, but there may not be the political will to finance the deployment of these solutions. There could be organizational constraints to prevent the distribution of information across public safety organizations.

- The workshop concluded that there is still lack of clarity in demand for interoperability. This lack of clarity is limiting the removal of the interoperability barriers, not the technology. There is a need to achieve a coherent message from the many different groups addressing differing aspects of interoperability.

- There is a need to develop realistic scenarios for interoperability (for law enforcement, crisis management, border control, etc) and associated business cases. EUROPOL and FRONTEX have been asked to take on this duty. Examples: cross-border operations, roaming across networks

- There is a need to define a strategy for providing broadband connectivity. Lack of harmonized use of frequency spectrum for PPDR in Europe (for wideband and broadband communications) is limiting production scale and future interoperability. Looking at the example of US, where the FCC has assigned 800MHz band, what scale of investment in dedicated PPDR broadband is justified for Europe?

- An important element is to minimize the impact of new technological solutions on existing infrastructures and networks. For example TETRA PMR gateways from some vendors do not have an impact on existing TETRA networks.

- Operational Research has a dominant contribution. Technology capabilities play an important supporting role. Operational incompatibilities can often be mitigated by technology. There is some evidence that full capabilities of TETRA/TETRAPOL are not being exploited

- In most cases, existing standards and technology capabilities can meet current interoperability needs but gaps are present. Gaps arise through lack of demand or fragmented information flow.

- Security is a mandatory requirement, but it can become an obstacle to security. For example, different national or organizational cryptographic policies can prevent communication and exchange of data even if the underlying network infrastructure is fully interoperable. An essential element to remove interoperability barriers is the alignment of the security policies across Europe.

- Value added services (situation awareness, video, location, and sensors) are on the threshold of rapid growth but there are not translated into specific requirements for broadband connectivity in Public Safety.

- The definition of future architectural options can be clarifying. It helps to indicate the need for ‘Innovation’ as well as ‘Research’.

- There is need to harmonize operational procedures and command practices to remove interoperability barriers including 24x7 communication command centres.

- There is a need to develop procurement approaches that enhance the competitiveness of EU industry. In this context interoperable secure communication has been recognized as potential lead market,

# 6. Recommendations from the workshop

## 6.1. Introduction

The workshop was concluded with a set of recommendations to identify actions and activities, which could benefit Public Safety organizations in the short term (2-3 years) and the long term (3-7 years).
For example, short term actions include activities from industry and government, which could develop and deploy technologies in the stage of maturity (e.g. gateway or technological evolutions of TETRA). Instead, long terms actions may include research activities from universities and research centres in industry and government, which investigate technical solutions still in their infancy.

A number of technological and research activities, which could be applied to the Public Safety domain, are in different stages of the technology lifecycle. Most of these technologies have been presented by the workshop participants in section 3.3. For a description of the various technological and research activities, please refer to Annex C. Key concepts in the technology lifecycle are invention and innovation. Invention is the development of a new idea that has useful applications. Innovation is a more complex term, referring to how an invention is brought into commercial usage.

We can identify the following phases of the technology lifecycle:

- Research: where new ideas are investigated in research centres but they are not deployed to the market yet. Neither the characteristics of technology nor its applicability to market needs may be well understood. Research role is predominant.
- Growth: where the technology start to be deployed in the market by one or more organizations. The size of the market is still limited or it is niche market. Research has still a role to improve efficiency in product development.
- Maturity: where the technology is widely deployed and it has reached market acceptance. Research activities are quite limited or non-existent.
- Decline: the technology is considered obsolete. Existing deployments are subsisted by new technologies.

The recommendations presented in the following paragraphs are related to technologies or approaches linked to one of the four phases described above.

It is also important to highlight that Public Safety communications may have various evolution paths. Depending on the evolution paths, research activities or technologies could be easily adopted, have limited adoption or not adopted at all.

We can identify the following evolution paths:

- **Slow incremental growth**. In this evolution path, working methods and infrastructures changes slowly. The deployment of new technologies is not encouraged and most of the efforts are dedicated to increase the efficiency of existing dedicated infrastructures. Availability of economical investment in the Public Safety sector is limited. Voice communications remains dominant. There is lack of political support for cross-border interoperability among Public Safety organizations of different member states. Public Safety network and commercial networks are separated. No new spectrum bands are allocated to Public Safety and for a limited amount (e.g. wideband).

- **Information driven growth.** In this evolution path, data communication is increasingly used to support voice communications. Wideband (i.e. up to 1 Mbits) communications is available and it is used to support a number of applications, including the creation of a "situational awareness picture" which can be shared among public safety officers in the field and in the control centres. Limited cross-border interoperability is available for voice and some data applications. There is limited use of commercial networks to support non-mission critical applications. Harmonized limited spectrum is allocated to Public Safety. There is a limited integration between commercial and public safety networks.

- **Full multimedia and convergent networks**. In this evolution path, data communication is the predominant form of communications and it is also used for mission critical applications. Political consensus is able to provide support for a significant improvement of public safety networks. Public Safety officers are used to conduct their operation on the basis of broadband applications like common operational picture. Interoperability barriers are removed through a number of technological solutions both a field level and among control centres. Innovative approaches for spectrum management allow a flexible use of the spectrum to accommodate needs of traffic capacity and broadband connectivity in the occurrence of emergency crisis or natural disasters. Commercial, military and public safety networks are fully integrated with resource management sharing solutions.

In these evolutions paths, a number of technologies can be used in various timeframes. Each technology will require different effort for research, development and deployment.
Figure 22 presents a hypothetical timeframe for the various technologies, which can provide *interoperability*. The horizontal axis is the time in years and the vertical axis provides an approximate estimate of the requested effort for research, development and deployment.

In a similar way, Figure 23 presents a hypothetical timeframe for the various technologies, which can provide *wideband or broadband connectivity*. The horizontal axis is the time in years and the vertical axis provides an approximate estimate of the requested effort for research, development and deployment.

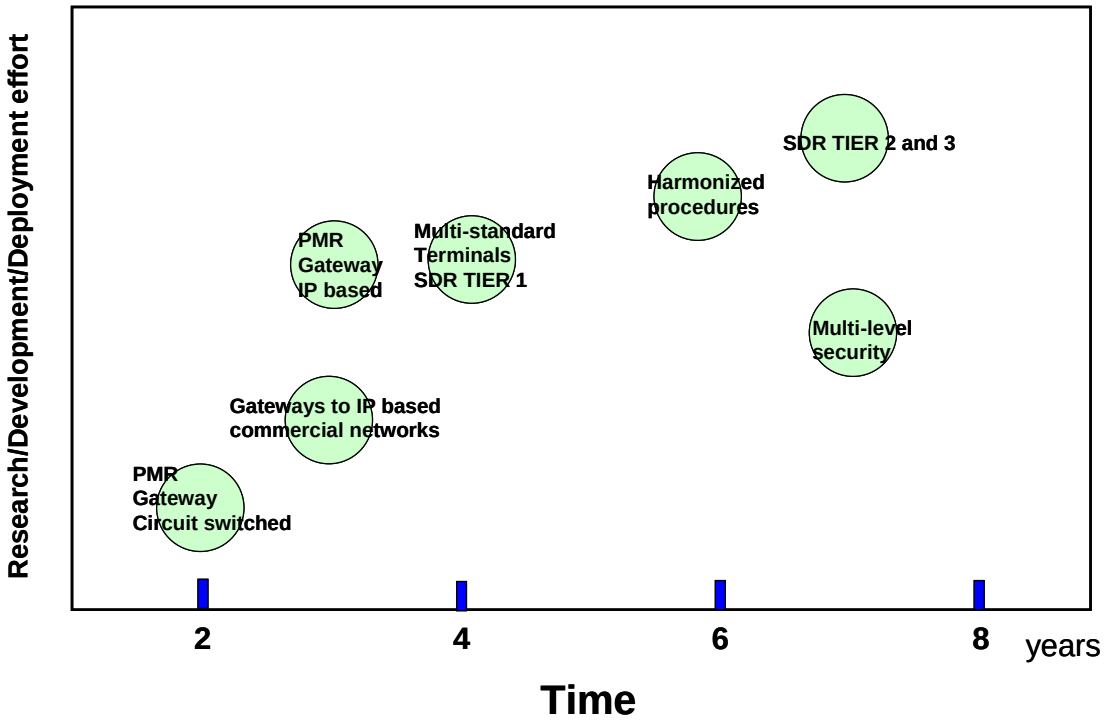


**Figure 22 Timeframe for Interoperability technologies**

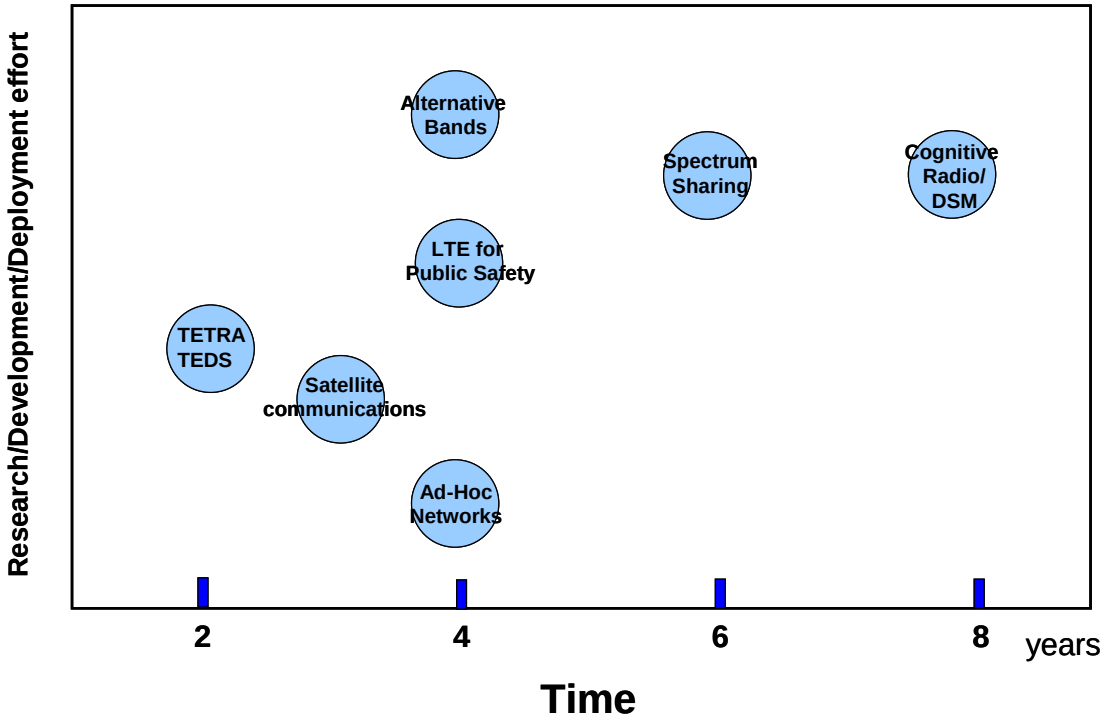


**Figure 23 Timeframe for Wideband/Broaband technologies**

Potential future architectures are described in Figure 24 and the potential research opportunities are shown in Figure 25:

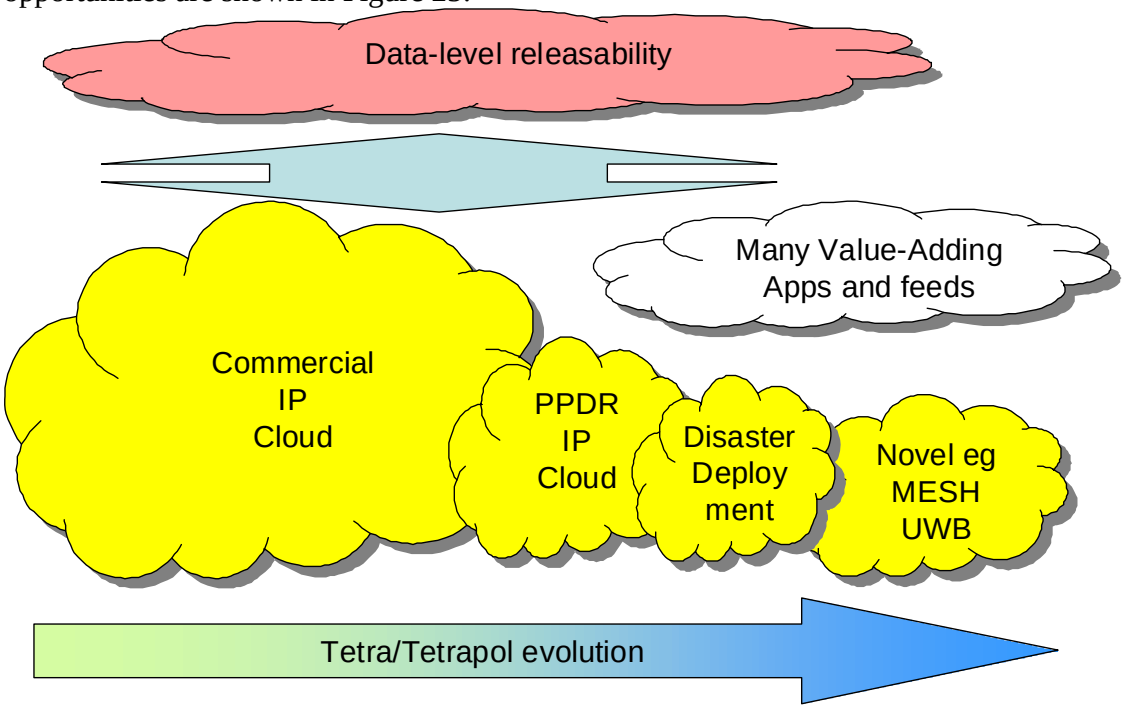


**Figure 24 Potential future architectures**

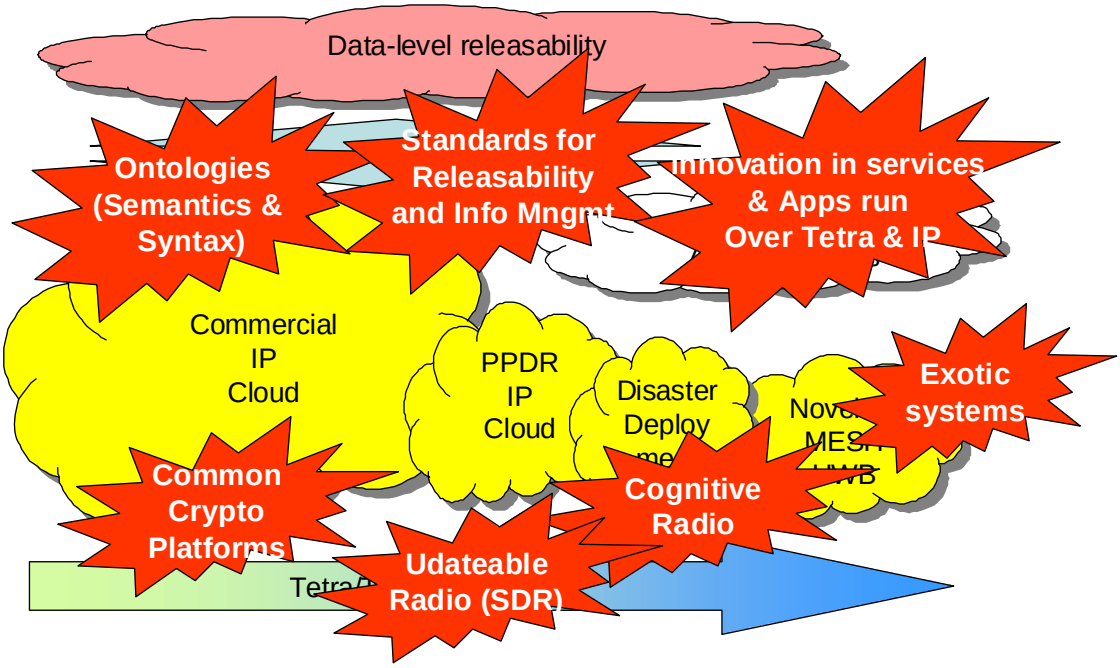


**Figure 25 Research opportunities**

## 6.2. Recommendations

The final session of the workshop focused on drawing together a set of recommendations. It was clear that many of the actions needed related to policy, process or procurement, whilst there were also important implications for technology research and development, especially to meet perceived requirements in the medium time frame (3-7 years).

The recommendations are therefore structured as four Groups:

- **Policy, Process or Procurement**
    1. Short Term Recommendations
    2. Medium Term Recommendations

- **Technology Development**
    1. Short Term Recommendations
    2. Medium Term Recommendations

### 6.2.1. Recommendations: Policy, Process Or Procurement (Short Term)

#### 6.2.1.1. Clarity over interoperability requirements and benefit.

There are many potential aspects to interoperability, and it would be unaffordable and probably undesirable to provide for arbitrary seamless interchange of information. The workshop concluded that whilst most potential user requirements for interoperability were already catered for in the technology standards, they were not always implemented or activated in actual systems. So while user needs had been expressed in the formulation of standards, these interoperability needs were not specified when procuring and operating communications systems.

A significant obstacle was lack of clarity in user system priorities, the benefits derived, and how to construct a business case to justify investment in interoperability functionality.

It was felt this should be addressed by exploring specific scenarios for interoperability (e.g. cross-border, roaming, disaster recovery, etc), to focus on the priority gaps in current capabilities. These scenarios would also provide evidence for the business case analysis to justify the investment in equipment or process change that would be implied. Quantitative models could be defined to support this analysis.

There was concern at the number of groups that were addressing different aspects of user needs for interoperability, and what authority they had.

***Recommendation 1.1: There should be an accepted approach at European level for prioritising user needs for interoperability, including the use of scenarios and business case construction. There is a need for a lead organisation to be 'custodian' for this requirement analysis, for example EUROPOL or FRONTEX, with the support of relevant organizations like the Law Enforcement Working Party (LEWP) Radio Expert group.***

#### 6.2.1.2. Harmonised procedures for creating communication groups, 'command doctrine' and training.

Experience of several nations in responding to crises emphasises the crucial role of support for managing communications interoperability. This includes real-time key management to define the cryptographically determined communication groups that are the fundamental feature of PPDR, making operational choices on the 'profiles' of system and security parameters, optimising gateways between systems, and maintaining priority settings. Where more than one nation or public service is involved, this will involve dynamic cooperation between these communications management centres. These functions can be called 'communications command' and require the same 24x7 availability as any other aspect of command.

Some nations already have such 24x7 functionality, some have it on a patchy basis, some have no real-time capability. Given the operational importance of interoperability, and the need to gain full value from the substantial investment made in communications technology, the provision of 24x7 communication controls should be adopted across Europe.

***Recommendation 1.2: 24x7 communication command centres should be made universal across public response systems***.

#### 6.2.1.3. Procure inter-system interfaces.

The TETRA standard provides for seamless, secure, interoperability between different TETRA systems, supporting setting up of groups of users across networks and provides for roaming across systems. To provide interoperability between different vendor networks, the ISI standard was established 10 years ago but it is based on old fashioned circuit-switching solutions. Although there are existing products based in this old technology, a very low demand from the user's side have limited so far their dissemination. Even if this requirement/need seems now more pregnant, some other new requirements have been added which could lead to a search for new technologies to cover the need to interconnect these systems intra-nationally and inter-nationally.

Note that there is a suggestion that the TETRA ISI standard should be updated to adopt current IP-based backbone carriers, something which could be achieved rapidly.

Consideration should be given to EU level pre-procurement funding to support development of a product that implements the TETRA ISI standard, or there should be an agreement between nations to share development costs, for example through a joint procurement programme. Industry would then have a defined market to respond to.

Interfacing between TETRA and TETRAPOL is a more difficult issue, with current solutions based on decrypted bridges without roaming being the only short term approach.

***Recommendation 1.3: Consideration should be given to EU level pre-procurement funding to support development of a product that implements the TETRA ISI standard or action should be taken across nations with TETRA systems to procure TETRA Inter System Interface equipment, so stimulating implementation of the ISI standard.***

#### 6.2.1.4. Review the strategy for wireless broad band for PPDR communications, especially for potential harmonisation of spectrum assignment.

Current TETRA and TETRAPOL networks provide limited data capacity, and with growth in various data services expected over the next decade, provision of enhanced data bandwidths comparable to civil mobile networks likely to become a priority. The Workshop expected a rising demand for bandwidth so that more frequency spectrum will be needed for PPDR. Given lead times and the costs implied by different approaches being taken, it is urgent that a strategy for Europe-wide PPDR wireless broadband is developed to avoid creating a fragmented outcome in later years.

There are several ways additional bandwidth could be provided:

- Deploy TEDS (an enhancement to TETRA), or TETRAPOL equivalent, in the existing PPDR frequency bands. This could provide an intermediate bandwidth, high availability solution, but existing bandwidth is already heavily used by voice services in many countries.
- Deploy TEDS in a new frequency band, preferably near the existing PPDR frequencies to enable existing base station infrastructure to be used.
- Deploy a true wireless broadband capability (e.g. LTE) in a new frequency band (as the US are doing at 800MHz)
- Use commercial mobile providers with pre-emption rights, perhaps supplemented by dedicated PPDR broadband in highly populated areas.

- A Europe wide strategy should be developed as a matter of urgency to map out which (combination?) of the above will be agreed.

***Recommendation 1.4. Conduct an urgent review to agree a Europe-wide strategy for provision of PPDR wireless broadband.***

## 6.2.2.Recommendations: Policy, Process Or Procurement (Medium Term)

### 6.2.2.1. Develop an 'Experimentation' environment to synthesize and explore future needs, especially those made possible by broadband connectivity.

Experience shows that provision of enhanced communication capabilities promotes new ways of working and behaviours that are impossible to predict. Defence experience shows that these can offer substantial improvements in performance, but generally emerge through people experimenting with new ideas, for example through trials and simulated rehearsal. This approach has been given the term 'Experimentation', as distinct from a formal requirements process, and has proved effective in finding the best ways to use new technology, especially where complementary evolution of processes and behaviour are necessary to capture the full value. With the need to generate better outcomes within resource constraints, finding ways to understand the impact of future technology will be important for PPDR.

Understanding the benefit from new technology will be especially important to justify the investment that would likely to be needed. For example, justifying investment in high bandwidth data over and above the current TETRA or TETRAPOL capabilities is proving difficult, even though there is an expectation that the return would be substantial in the medium term.

***Recommendation 1.5: Create Experimentation facilities to accelerate innovation between technology and users, and explore new ways of gaining benefit from technology.***

### 6.2.2.2. Review information sharing policy.

Security policies between nations are a significant limitation to achieving interoperability. There is a vital need to protect sensitive information and necessarily requires control of access and some use of sovereign cryptographic algorithms. The TETRA and TETRAPOL systems that replace previous public safety

communications systems have many more controls on voice and data access can enable security policies to be more selective in terms of user group and operational context as to what can be shared.

There is an opportunity to review and where possible harmonise information sharing polices, moving from the legacy of a ‘system-high’ approach to security to a richer model where sharing properties are designated at the level of data items or conversations. This is likely to imply significant changes to procedures about how information items are created and managed in terms of their need to be shared.

***Recommendation 1.6: Explore harmonising a shift towards managing access to data on the basis of ‘shareability’ properties, rather than just levels of classification.***

### 6.2.3. Recommendations For Technology Development (Short Term)

#### 6.2.3.1. Examine feasibility for dual standard TETRA/TETRAPOL handsets.

Interoperability between handsets of different standards can only be provided by overlapping, bridged networks as has been deployed in some border areas, or locally through DMO. More general interoperability, for example roaming, can only be achieved through dual standard appliances. Many recent PPDR radios use a similar internal architecture for both standards, the differing technical protocols being implemented in firmware. It may therefore be feasible for manufactures to produce a dual standard option at an affordable price, or even upgrade existing appliances with new firmware.

***Recommendation 2.1: Commission a feasibility study to assess options for bringing dual standard handsets to the market, and resolve any licensing issue this might imply.***

#### 6.2.3.2. Establish a formal, overarching process for agreeing standards and profiles across PPDR communications systems.

Technical standards are currently developed by separate bodies focused in TETRA or TETRAPOL communities. These technical standards define the capabilities of the systems, but not the way the various system and operational parameters (or 'profiles') are set for individual systems. There is a need for an overarching body that can harmonise the profiles across systems and also agree optimum means for achieving interoperability between TETRA and TETRAPOL networks. Such a body might have a growing role in defining data standards as the need for consistent data semantics grows, and to exploit into PPDR the much faster moving standards that are emerging from commercial mobile services. This role would be similar to that of the Internet Engineering Task Force, and might be carried out by the Law Enforcement Working Party (LEWP) in conjunction with ETSI and CEN.

***Recommendation 2.2: Make formal a cross-system role for evolving and defining harmonised profiles and data standards.***

## 6.2.4. Recommendations For Technology Development (Medium Term)

### 6.2.4.1. Collaborative research to develop new PPDR communications functionality

The concept of experimentation facilities can be further extended to create collaborative research facilities to bring together users, research and industry in a specific application domain (e.g. Public Safety communications) to steer research stimulate new ways of working. This is the concept of "Living Lab", which is represented in Europe by European Network of Living Labs (ENoLL). From [18], "the European Network of Living Labs (ENoLL) is a community of Living Labs with a sustainable strategy for enhancing innovation on a systematic basis. The overall objective is to contribute to the creation of a dynamic European innovation system. ENoLL aims to support co-creative, human-centric and user-driven research; development and innovation in order to better cater for people's needs".

***Recommendation 2.3: Establish a new research area for ENoLL in the area of Public Safety.***

### 6.2.4.2. Support research aimed at exploiting cognitive radio and software defined radio in PPDR networks.

A feature of PPDR communications is the high peak traffic volumes at time of crises or during major events. New spectrum management approaches based on cognitive radio and software defined radio can improve the spectrum utilization and provide the additional traffic capacity and broadband connectivity in time of crisis to Public Safety organizations. Cognitive radio as a concept is consistent with the shift in frequency spectrum management approach away from static assignments towards greater real-time flexibility. An especially relevant example for PPDR would be sharing with adjacent military frequency allocations. There is the need to investigate these technologies for deployment in PPDR domain and identify their benefits and shortcomings.

While promising, Cognitive Radio is still in the "research" phase in the Public Safety domain and early "growth" phase in the Commercial domain where standards have already been defined (i.e. IEEE 802.22) and early prototypes/products have been implemented.

There are a number of challenges to address:

- The cost and complexity of cognitive radio technology is still very high for an effective deployment of this technology in the Public Safety domain.

- Cognitive radio technology must satisfy the requirement of reliability, availability and security already defined for Public Safety dedicated networks (e.g. TETRA).
- New organization structures and procedures must be defined to use the shared spectrum in case of emergency crisis.
- The new spectrum management approach must be discussed and approved by European spectrum regulators.
- The introduction of cognitive radio technology should minimize the impact on existing Public Safety networks.

Cognitive radio used in this way raises technological, operational and legal issues, and therefore needs further research across all these aspects before it could be deployed on a mature basis. It also needs technology development, much of this drawing from software defined radio research being conducted for other (e.g. military) objectives.

***Recommendation 2.4: Initiate research into the practical issues of deploying cognitive radio in the PPDR context.***

#### 6.2.4.3. Adopt an open innovation approach to provide fast moving services.

The Workshop exposed a variety of opportunities for extensive use of data which would greatly aid effectiveness and efficiency of PPDR organisations. The ability to access and share information, to tailor data to specific needs, and maintain situation awareness opens many new potential uses of data and the services that support them. As for the Internet, it is not always possible to predict the nature and benefit from such services, and an open environment where third parties can offer information applications and services through the network providers would stimulate rapid innovation in this area. The concept would be more like the regulated ‘appstores’ available for mobile phones, rather than exclusive provision by a network service provider.

***Recommendation 2.5: Adopt an open innovation approach to provision of new PPDR information based services.***

## 6.3. Summary of recommendations

In Figure 26 and Figure 27, we compare the recommendations to the PPDR challenges described in 2.1.

| | Interoperability | Broadband Connectivity | Lack of coverage | Degraded infrastructures | Technological gap |
|---|---|---|---|---|---|
| Recommendation 1.1: Prioritising user needs for interoperability |  |  |  |  |  |
| Recommendation 1.2: Harmonised procedures |  |  |  |  |  |
| Recommendation 1.3: Procurement of Inter System Interfaces |  |  |  |  |  |
| Recommendation 1.4: European strategy for Broadband PPDR communications |  |  |  |  |  |
| Recommendation 1.5: Create Experimentation facilities |  |  |  |  |  |
| Recommendation 1.6: Information sharing policy |  |  |  |  |  |

**Figure 26 Policy, Process or Procurement**

| | Interoperability | Broadband Connectivity | Lack of coverage | Degraded infrastructures | Technological gap |
|---|---|---|---|---|---|
| Recommendation 2.1: Dual standard handsets |  |  |  |  |  |
| Recommendation 2.2: Cross-system role for evolving harmonised standards |  |  |  |  |  |
| Recommendation 2.3: Collaborative Research |  |  |  |  |  |
| Recommendation 2.4: SDR/CR in PPDR |  |  |  |  |  |
| Recommendation 2.5: Innovation approach in PPDR |  |  |  |  |  |

**Figure 27 Technology Development**

# References


[1] SAFECOM, US communications program of the Department of Homeland Security. “Public safety Statements of Requirements for communications and interoperability v I and II”. http://www.safecomprogram.gov.

[2] United States Government Accountability Office. Report to the Chairman, Subcommittee on Communications, Technology, and the Internet, Committee on Commerce, Science & Transportation, United States Senate on Emergency Communications. GAO-09-604.

[3] Terms of Reference for Specialist Task Force STF RRS/TETRA (TC RRS WG 4 /TC TETRA WG 4) on” Configuration of Reconfigurable Radio Systems in future Public Safety & Security Systems (PSS) in a Public Protection and Disaster Relief (PPDR) network”.

[4] INTER-SYSTEM INTERFACE, List of Requirements.V1.0. BDBOS – A.S.T.R.I.D. – VTS PN.

[5] Use Cases for Cognitive Applications in Public Safety Communications Systems - Volume 1: Review of the 7 July Bombing of the London Underground (http://www.sdrforum.org/pages/documentLibrary/documents/SDRF-07-P-0019-V1_0_0.pdf)

[6] D3.13 - Market Issues PROJECT No 034895 NARTUS / PSCE Public Safety Communication Europe.

[7] ETSI TC RRS Reconfigurable Radio Systems (RRS). System Aspects for Public Safety. ETSI TR 102 733.

[8] ETSI TC RRS Reconfigurable Radio Systems (RRS). User Requirements for Public Safety. TR 102 745.

[9] Draft Council Recommendation on improving communication between operational units in border areas. Council of the European Union Brussels, 3 October 2008. 13716/08 ENFOPOL 176 COMIX 690.

[10] Federal Communications Commission. National Broadband Plan. Accessible at http://download.broadband.gov/plan/national-broadband-plan.pdf. Chapter 16: Public Safety.

[11] FP7 EULER project. http://www.euler-project.eu/.

[12] FP7 SECRICOM project. http://www.secricom.eu/

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

[14] Public Protection and Disaster Relief Spectrum Requirements. Helsinki, January 2007. Electronic Communications Committee (ECC) within the European Conference of Postal and Telecommunications Administrations (CEPT).

[15] V.K. Narayanan, Managing Technology and Innovation for Competitive Advantage. Prentice-Hall, Inc., August 19, 2000.

[16] Draft TS/EMTEL 102 181 “Requirements to Communications between Authorities”.

[17] OASIS http://www.oasis-open.org/specs/index.php#capv1.1

[18] The European Network of Living Labs (ENoLL). http://www.openlivinglabs.eu/
[19] Chesbrough, H.W. (2003). Open Innovation: The new imperative for creating and profiting from technology. Boston: Harvard Business School Press.
[20] PASR 2006 WINTSEC project. http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/06/375.
[21] Wireless Innovation Forum. http://www.wirelessinnovation.org. Last accessed 12/04/2010.

# Annexes

## A. Public Safety organizations and functions

## A.1. Introduction

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 defence 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. Because of such diversity, this technical report will not try to classify the various Public Safety organizations across Europe. The approach, adopted in this annex, is to define taxonomy of the main responsibilities and functions of public safety organizations.
The report will then provide, for information purpose, a mapping of existing public safety organizations to defined functions and responsibilities.

The following functions are defined:

- Law Enforcement
- Emergency Medical Services
- Border Security
- Protection of the environment
- Search and rescue.

These basic functions and the associated roles will be described in details in the following paragraphs.
In this report, private organizations with similar structure and activities of public safety organizations will not be considered. For example private guard organizations of a business company.
Most of the information presented in this chapter is extracted from ETSI TR 102 745 "User Requirements for Public Safety" produced by ETSI TC RRS.

## A.2. Public Safety functions

### A.2.1. 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 offences 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 offence 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 offence against customs law (this function is also shared by border security).
- Law enforcement in the transportation domain to identify law offences on the transportation infrastructures like road, air, railways and sea.
- Custody and transportation of criminal convicts.

### A.2.2. Emergency Medical services

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.

### A.2.3. 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 offence of customs laws.

### A.2.4. 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.

### A.2.5. 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

### A.2.6. 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.

### A.2.7. 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.

## A.3. Public safety organizations and functions

Table 1 provides the overview of the various public safety organizations, their description and the functions they usually perform.

| Public Safety Organization | Description | Functions |
|---|---|---|
| Police | The main objective of the police is law enforcement creating a safer environment for its citizen. | Law enforcement |
| Fire Services | With variations from region to region and country to country, the primary areas of responsibility of the fire services include:<br>• structure fire-fighting and fire safety;<br>• wild land fire fighting;<br>• life saving through search and rescue;<br>• rendering humanitarian services;<br>• management of hazardous materials and protecting the environment;<br>• salvage and damage control;<br>• safety management within an inner cordon;<br>• mass decontamination. | Law enforcement, protection of the environment, search & rescue |
| Border Guard (Land) | Border Guard organizations 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 |
| 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 |
| 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. |
| 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 |
| Military | Military is the organization responsible for the national defence 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 |
| 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 |
| 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 |
| 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 |
| Airport Security | Airport enforcement authority is responsible for protecting | Law enforcement |

| Public Safety Organization | Description | Functions |
|---|---|---|
| | airports, passengers and aircrafts from crime. | |
| Port Security | Port enforcement authority is responsible for protecting port and maritime harbour facilities. | Law enforcement |
| 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. |

**Table 1 Public Safety organizations and functions.**

## B. Public Safety applications

This section lists the current and future PPDR applications, which will drive the need for broadband connectivity in the future:

- *Verification of biometric data*. Public Safety officers may check the biometric data of potential criminals (e.g. fingerprints) during their patrolling duty. The biometric data could be transmitted in real-time to the command control centre for verification.
- *Mobile command centr*e. Decentralized command centres can be deployed in the field and they need to maintain constant communication with the headquarters to access mail and intranets, transmit incident reports, and download relevant data and so on.
- *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 & control centres.
- Support for *ad-hoc sensor network*s deployed in the crisis area or along the border. The collected data can include information on the environment like temperature or poisonous gas or images.
- *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 or another Id document in a more efficient way.
- *Applications for location and guiding (AVL)*. Controls room should have the position of all the officers in the field like vehicles and people. AVL does already exist today but some features are still missing like the capability of sending AVL to the officers themselves or integrate the AVLs of various organizations.
- *Database access and checks.* This application area includes all the activities where public safety officers must retrieve data from the headquarters to support their work.
- *Transmission of Building/Floor plans*. 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. Building or floor plans can be requested to the headquarters and transmitted to the public safety responders.

- *Monitoring of vital signs of Public Safety officers*. This is particularly important for fire-fighters and officers involved in dangerous operations (e.g. search & rescue during a fire).
- *Remote emergency medical services*. Through transmission of video and data, medical personnel may intervene or support the team in the field for an emergency patient.
- Collect and share the *common situation picture* among Public Safety responders of various organizations. The common situation picture created in the field or at the control centre can be re-distributed to the officers in the field.
- *Access to digital maps*. Public Safety officers in the field can access aerial photographs, satellite images & maps. Because, digital maps have usually high resolution, communication systems must provide broadband connectivity for this application.
- *Remotely controlled devices*. Robots or drones can be used in environment where the risk for humans is too high. Communications are needed to guide the robotics devices or to retrieve the information collected from the devices. For example, the robots could be equipped with a video camera or radar systems.

Each application can have different requirements in terms of broadband connectivity, range, security, interoperability and reliability.

Table describes the needs of the previous applications in terms of the Public Safety requirements.

We can identify the following specific requirements for Public Safety communication systems:

- **Interoperability**, which can be defined as the capability to communicate and distributed information across different wireless communications systems used by different public safety organizations. Interoperability includes the internetworking functionality. In the table, interoperability could have the values: *Necessary* (full interoperability is needed), *Limited* (only basic interoperability functions are needed), *Not Necessary*.
- **Timeliness**, which can be defined as the capability to setup a connection or deliver message and data in a specific time (e.g. 250 ms for connection set-up). Timeliness can have the values *High* (less than 250 ms), *Medium* (less than 10 seconds) and *Not needed* (not constraints).
- **Coverage**, which can be defined as the area over which reliable communication can be established and maintained. Public Safety organizations must have wide coverage to be able to address request of help in any area. In the table, coverage can be *Wide* (tens of Kms radius), *Medium* (1-4 Km radius) and *Local* (up to 1 Km radius).

- **QoS**, which can be defined as measure of the parameters of a network that influence perceived quality of communications, including the delay, jitter, bandwidth, and packet loss that packets sent by the application experience when being transferred by the network. In the table, QoS can be *High* (TETRA compliant), *Medium* (commercial WLAN) and *Best Effort.*

- **Throughput**, which can be defined parameter that defines the effective network data transfer rate in bits per second (bps) for a particular service. In the table, throughput can be *Broadband* (above 1 Mbits), *Wideband* (hundred of Kbits) and *Narrowband* (tens of Kbits)

Similar data is presented in references [8], [13] and [16].

**Table 2 Applications and related requirements**

| Application | Throughput | Interoperability | Timeliness | QoS | Coverage |
|---|---|---|---|---|---|
| Verification of biometric data | Wideband | Necessary | Medium | High | Low |
| Mobile command centres | Broadband | Necessary | Medium | High | Wide |
| Wireless video surveillance and remote monitoring | Broadband | Limited | High | High | From Medium to Wide |
| Ad-hoc sensor networks | Wideband | Limited | Medium | Medium | Local |
| Automatic number plate recognition | Wideband | Not Necessary | Medium | High | Wide |
| Documents scan | Wideband | Limited | Medium | High | Local |
| Applications for location and guiding (AVL) | Narrowband | Necessary | High | Medium | Wide |
| Database access and checks. | Wideband | Limited | Medium | Medium | Wide |
| Transmission of Building/Floor plans. | Wideband | Limited | Medium | High | Wide |
| Monitoring of vital signs of Public Safety officers | Narrowband | Limited | High | High | Local |
| Remote emergency medical services | Wideband to Broadband | Necessary | High | High | Wide |
| Common situation picture | Wideband | Necessary | High | Medium | Wide |
| Access to digital maps. | Broadband | Necessary | High | Medium | Wide |
| Remotely controlled devices. | Wideband | Limited | High | Medium | Local |

# C. Research Areas and Technologies

The purpose of this Annex is to describe in more detail the main research areas and technologies, discussed during the workshop and how they are related to the Public Safety domain.

## C.1. Software Defined Radio

Software defined radio uses programmable digital devices to perform the signal processing necessary to transmit and receive base band information at radio frequency. Devices such as digital signal processors (DSPs) and field programmable gate arrays (FPGAs) use software to provide them with the required signal processing functionality. This technology offers greater flexibility and potentially longer product life, since the radio can be upgraded very cost effectively with software.

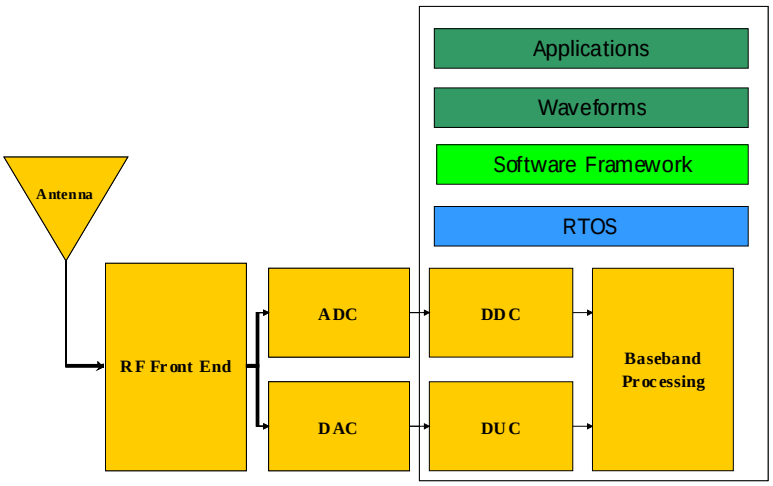


**Figure 28 Software Defined Radio**

From the technological point of view SDR was born as a military project (JTRS) of the US DoD aiming at standardizing the core of the radio equipments used by the different branches of the military forces in order to reduce the cost, improve interoperability and increase the upgradeability.

As investigated in the WINTSEC [20] and EULER [11] projects, SDR can be used to remove the interoperability barriers by provide terminals and base stations, which can connect to different communication systems based on different standards.

There are different definitions of SDR, which may include devices of various technological sophistication.

Wireless Innovation Forum in its previous incarnation as Software Defined Radio Forum defined five tiers of SDR. While this definition may be obsolete, it provides a description of the potential technological implementations of SDR.

- Tier 0 – Hardware Radio, which is a baseline radio with fixed functionality.
- Tier 1 – Software-Controlled Radio, where the radio's signal path is implemented using application specific hardware.
- Tier 2 – Software Defined Radio, where most of the radio functions are performed in software. For example, the signal path can be reconfigured in software without requiring hardware modifications.
- Tier 3 – Ideal Software Radio, where software programmability extends to entire system.
- Tier 4 – Ultimate Software Radio, which has full programmability, may operate in a broad range of frequencies and can switch from one air interface/application to another in a limited time (e.g. milliseconds).

While SDR of type 3 and may be deployed in the Public Safety market only 10 years or more in the future, Tier 1 and 2 may have a potential application in the near term (3-5 years).

## C.2. Cognitive Radio

In ETSI, a CR radio is defined as "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".

It is usually recognized that CRs should provide the following functions:

- determine which portions of the spectrum are available and detect the presence of licensed users when a user operates in a licensed band (spectrum sensing),
- select the best available channel (spectrum management) for communication,
- coordinate access to this channel with other users (spectrum sharing), and
- vacate the channel when a licensed user is detected (spectrum mobility).

To date, the applicability of CR to Public Safety communications with their specific requirements regarding availability, access time, reliability, etc. has not yet been sufficiently verified. Some technical obstacles, like e.g. the hidden node problem, still have to be overcome.
Therefore, it is likely that, in an evolutionary approach, cognitive radio concepts will initially be used for other, less complex functions like for example Public Safety coverage enhancements.
A preliminary proposal for the application of CR to Public Safety could be based on two layers approach.

- A static allocation of the spectrum is used for basic services like voice and narrowband communication and messaging.
- A dynamic allocation of the spectrum is used to provide broadband connectivity. Dynamic spectrum allocation can be based on the concept of spectrum sharing with commercial providers. In case of emergency, commercial providers will shut down their communication systems and free their spectrum bands. Public Safety CR nodes will be able communicate and transmit in these spectrum bands for the duration of the emergency crisis.

There are a number of issues with this approach:

- Some public safety organizations may consider basic services event high data messaging services, as they would be essential for their activities.
- Who will guarantee that commercial providers will promptly shut down their networks in case of emergency? The risk is that some commercial providers will still transmit in the shared spectrum bands and they will create interference to CR-based public safety communication systems.
- Commercial networks are still needed in case of emergency crisis to alert the population through broadcast communication and messages. A specific amount of spectrum resources must be available to commercial networks to alert the civilian population. Some NGO organizations do also use commercial networks and they participate to the resolution of the emergency crisis.

## C.3. Ad-hoc Networks

A mobile ad hoc network (MANET) represents a system of wireless mobile nodes that can freely and dynamically self-organize into arbitrary and temporary network topologies, allowing people and devices to seamlessly internetwork in areas without any pre-existing communication infrastructure. While many challenges remain to be resolved before large scale MANETs can be widely deployed, small-scale mobile ad hoc networks will soon appear. Network cards for single-hop ad hoc wireless networks are already on the market, and these technologies constitute the building blocks to construct small-scale ad hoc networks that extend the range of single-hop wireless technologies to few kilometres.

Ad-hoc networks can be deployed for Public Safety uses for a variety of applications including monitoring of the environment, body area networks, improve the coordination of the first time responders and so on. Ad-hoc networks can be based on existing Public Safety communications technologies like TETRA DMO or by tailoring commercial or military networks like WiFi or Tactical networks.

## C.4. Sensor Networks

A wireless sensor network consists of a possibly large number of wireless devices able to take environmental measurements. Typical examples include temperature light, sound,

and humidity. These sensor readings are transmitted over a wireless channel to a running application that makes decisions based on these sensor readings.
Many applications have been proposed for wireless sensor networks, and many of these applications have specific quality of service (QoS) requirements that offer additional challenges to the designer. One widely recognized issue is the limited power available to each wireless sensor node, but other challenges such as limited storage or processing capabilities play a significant role in constraining the application development.

Sensor networks have a number of applications in the Public Safety domain. They can be deployed to detect forest fires or movements of the earth in case of earthquake or avalanche or to monitor the environment as a consequence of a flooding. In the Public Safety domain, security, resilience and energy efficiency aspects are particularly important in comparison to other application domains and this where most of the research efforts should be targeted.

## C.5. RFID

Tags, a reader/writer and a host system compose a typical RFID system. An RFID tag is usually of very small size and low cost device, so that it can be easily implanted on a physical object like a product, a box or even an animal or a person. A RFID tag is composed by tiny electronic circuits able to store and process a limited amount of data (from several bits to several kilobytes) and by a miniature antenna for short-range wireless communication.
RFID tags are classified as passive or active. Passive tags work by taking the energy received from the reader through the tags antenna and using that energy to transmit stored data back to the reader. Passive tags are less expensive than active tags, which include their own power supply, usually a battery, to transmit information directly to a reader. The battery can also be used to help power or interact with other devices. For example, a company shipping perishable goods may want to use active tags that integrate with thermometers to ensure the goods are kept at an acceptable temperature.

RFID can be used in various emergency crisis scenarios to tag the goods shipped to the disaster areas. Security is an important requirement as goods could be tampered or stolen. The use of secure RFID is recommended.

## C.6. Operational research

Operational Research (OR) is the discipline of applying advanced analytical methods to help make better decisions. Researcher and professionals aim to provide rational bases for decision making by seeking to understand and structure complex situations and to use this understanding to predict system behaviour and improve system performance. Operational research is implemented through analytical and numerical techniques to develop and manipulate mathematical and computer models of organizational systems composed of people, machines, and procedures.

The origins of Operational Research are in the defence before and during World War II.

The application of OR is not new, as decision support systems, using concepts of OR, are used in command and control centres of Public Safety organizations. Disaster supply chain or AVL during a natural disaster are typical scenarios where OR has been already applied.

There are still many Public Safety areas where OR can be applied including the case of interoperable organizations with different level of authority and security, investigation of the impact of new applications (e.g. AVL) and so on.

## C.7. Human-machine interface

Human-Computer Interfaces (HCI) is the study of interaction between people (users) and computers. HCI research is essential to improve the usability of the terminal and equipment used by Public Safety forces. As described in 3.3.4, usability is still a major concern for Public Safety officers.

There are a number of specific research areas, which can be applied to Public Safety including Multimodal User Interaction (MMUI), where not only voice, but also gestures, facial expression and other body languages can be used to facilitate user's interaction with the computer and improve tasks efficiency and user experience.

Another area is to align to investigate how HCI in public safety will change when interoperability solutions will be able. The capability of accessing data outside the conventional domain will have an impact on the existing machine interfaces.

## C.8. Multi-level security

Public Safety organizations may have different levels of security for the transmission and storage of data. While some organizations should interact with defence organizations during natural disasters, NGOs may not have security requirements or mechanism in their networks. As described in the report, security can become a barrier to interoperability, as Public Safety organizations may not have the will to share information with other organizations even if they have the technical capabilities (e.g. interoperable networks).

This is a common problem in defence networks, where a red and black networks are set-up to provide different level of security. In most case, these networks are physically separated.

An interesting research is multi-level security, which investigates the capability of providing access and distribution of data with different levels of security. This research activity may have important outcomes for the Public Safety domain.
Challenges for research are:

- Multi-level security may be quite expensive to design and deploy.

- Multi-level security often requires centralized architecture. How this requirements fits with the organizational structures or Public Safety organizations.
- The impact of multi-level security on public safety network should be minimized.

## C.9. Mobile ID

Mobile Id devices are mobile terminals, which gather, process and transmit an individual's biometric data—fingerprints, facial and iris images—for identification.
Mobile Id devices can be implemented in personal digital assistants (PDAs), ultra-portable personal computers, PPDR terminals (e.g. TETRA) or other devices, which are portable and they had the capacity to acquire images, process them and transmit to a remote station or control centre. Mobile Id devices may be employed for a variety of applications, where stationary booking station type environment is not possible, nor easily attainable including:

- Mobile immigration and border control needs in non stationary environments.
- Identification and verification in law enforcement applications. For example, control of identity documents in trains or bus.
- Access control for buildings, computers and networks in flexible application environments.

## C.10. Next Generation fixed networks (NGN)

A Next Generation Network (NGN) is a packet-based network able to provide services including Telecommunication Services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It offers unrestricted access by users to different service providers. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users (from ITU).

NGN networks will be mostly based on IP. As Public Safety networks will move towards an NGN approach and technologies, it is important to investigate the impact on the existing networks and operational procedures. Will NGN be able to satisfy Public Safety requirements ? How prioritization of the services can be implemented ? How to design NGN gateway bridges with connect control centres of different Public Safety organizations.

This area is not only research but also standardization activity.

## C.11. Next generation wireless networks (LTE)

(From http://www.3gpp.org/About-3GPP) "The original scope of 3GPP was to produce Technical Specifications and Technical Reports for a 3G Mobile System based on

evolved GSM core networks and the radio access technologies that they support (i.e., Universal Terrestrial Radio Access (UTRA) both Frequency Division Duplex (FDD) and Time Division Duplex (TDD) modes). The scope was subsequently amended to include the maintenance and development of the Global System for Mobile communication (GSM) Technical Specifications and Technical Reports including evolved radio access technologies (e.g. General Packet Radio Service (GPRS) and Enhanced Data rates for GSM Evolution (EDGE)). 3GPP was created in December 1998 by the signing of the "The 3rd Generation Partnership Project Agreement". The latest 3GPP Scope and Objectives document has evolved from this original Agreement".

Long Term Evolution (LTE) represents the next generation of wireless networks, able to provide broadband connectivity and a large set of services. As described in ETSI, The Third Generation Partnership Project deals with a number of 3G services dedicated to public safety: the Priority Service and Multimedia Priority Service, the Voice Group Call Service (VGCS) for public authority officials, the transferring of emergency call data and the Public Warning System.

It is quite likely that LTE networks will be used to complement Public Safety dedicated networks (e.g. TETRA) to provide broadband connectivity as described in 3.3.23.

This will imply the use of terminals able to interface both Public Safety dedicated networks and LTE networks.

## C.12. Satellite Communications

Satellite communications have already been used to support Public Safety operations and emergency organizations as they have the unique feature that they do not need ground infrastructures in the disaster area. Of the most likely outcome of a natural disaster like an earthquake or flooding is the degradation or destruction of the ground wireless infrastructure. Even if dedicated Public Safety networks are particularly resilient against this type of disaster due to High Availability solutions, satellite communications is the only communication system, which may provide broadband communications in the absence of a ground wireless infrastructure. HF communication can also provide coverage for very large areas, but it only provides very limited data connectivity.

Satellite communication can already provide broadband connectivity as described in 3.3.15.
Future research trends can explore improvement in the performance and efficiency of the broadband communications offered by satellite systems.

European Commission

EUR 24540 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen

# Report of the workshop on “Interoperable communications for Safety and Security”
28/29 June 2010 – Ispra, Italy.
Workshop jointly organized by DG ENTR and DG JRC with the support of EUROPOL and FRONTEX.

Gianmarco Baldini
Luxembourg: Publications Office of the European Union
2010 – 89 pp. – 21 x 29.7 cm
EUR – Scientific and Technical Research series – ISSN 1018-5593
ISBN 978-92-79-16921-2
doi:10.2788/19075

Abstract
Public Protection and Disaster Relief (PPDR) services bring value to society by creating a stable and secure environment. The provision of adequate capabilities to PPDR organizations and its officers is a priority subject for citizens, National Governments and the European Union. The protection to be ensured by the PPDR primarily covers people but also the environment and property, and it address a large number of threats both natural and man-made, acts of terrorism, technological, radiological or environmental accidents, occurring inside or outside the EU. Telecommunications technologies provide the capability of exchanging information (e.g. voice or data) to connect all the involved parties in the crisis and to coordinate the relief efforts. In the field, wireless communications have an essential role to support the mobility of first time responders by providing continuous connectivity among responders and with the headquarters.

Wireless communications can support first time responders in a variety of operational tasks including:

- Maintain voice communication to coordinate the relief efforts for the resolution of the crisis.
- Creation and distribution of a Common Operational Picture among all the responsible parties.
- Collect and distribute data on the operational context or the environment from sensors.
- Retrieve data from central repositories (e.g. building plans, inventory data) to support their activity.
- Support the tracking and tracing of the supply chain of goods and materials needed in the response and recovery phases of a crisis.

To support these tasks, telecommunications must be reliable, secure and provide minimal levels of Quality of Service (QoS). Misinterpretations can cause loss of life or delay the resolution of the disaster. In Europe, many dedicated network infrastructures have been built and deployed to provide the necessary capabilities for PPDR organizations. There are still a number of challenges to be resolved through the combined efforts of government, industry, end-users and research.

On the 28th and 29th June 2010, DG ENTR together with DG JRC and with the support of EUROPOL and FRONTEX has organized a workshop to identify the main challenges in the European PPDR context and describe the research activities to address and resolve such challenges. Regulations and standardization play an important role in applying the results of research to the market and to the PPDR end-users. The workshop has seen a large participation of representatives from the government, standardization, industry and PPDR end-users. The workshop has identified research gaps and it has defined a number of recommendations, where action at European level should be taken.

The purpose of this report is to describe the findings of the workshop and the related recommendations.

How to obtain EU publications

Our priced publications are available from EU Bookshop (http://bookshop.europa.eu), where you can place an order with the sales agent of your choice.

The Publications Office has a worldwide network of sales agents. You can obtain their contact details by sending a fax to (352) 29 29-42758.

The mission of the JRC is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies. As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.

JRC

EUROPEAN COMMISSION

LB-NA-24540-EN-C

Publications Office

ISBN 978-92-79-16921-2