The Evolution of ICT in the Public Safety Domain: Challenges and Opportunities

Gianmarco Baldini [1], Oriol Sallent [2], Sebastian Subik [3], Christian Wietfeld [3]

[1] *Joint Research Center of the European Commission, Ispra, Italy*

[2] *Universitat Politècnica de Catalunya (UPC), Spain*

[3] *Communication Networks Institute, TU Dortmund University, Germany*

gianmarco.baldini@jrc.ec.europa.eu, sallent@tsc.upc.edu, sebastian.subik@tu-dortmund.de, christian.wietfeld@tu-dortmund.de

Abstract

The services provided by public safety organizations bring value to society by creating a stable and secure environment. These services include protection to people and assets and they address a large number of threats both natural and man-made, including acts of terrorism, technological, radiological or environmental accidents. Information and Communication Technologies (ICT) have always played an important role in the public safety domain. The capability of exchanging information (e.g., voice or data) is essential to improve the coordination of public safety officers during an emergency crisis. Wireless communications are particularly important in field operations to support the mobility of first responders. Operational and business requirements in the public safety domain are significantly different from the commercial domain. Innovative ICT concepts and technologies may not be directly applicable to the public safety domain or they need to be customized to validate specific requirements of Public Safety organizations (e.g., security).

This paper will identify the most significant challenges in the Public Safey domain, the main technical enablers and the opportunities provided by new ICT technologies. In particular, this paper focuses on the lack of interoperability and broadband connectivity for public safety organizations. The potential evolution paths for ICT in the public safety domain will also be described.

Keywords: *ICT, Wireless Communications, Security, Public Safety*

1. Introduction

Information and Communication technologies have always been part of the history of the Public Safety (PS) domain. As in the commercial and military domain, users need to collect, analyze, distribute and store information among various entities and different contexts. The challenge of crisis management or disaster management is to reduce the impact and injury to individuals, assets and the society. This task requires a set of capabilities, which includes communication, resource management, supply chain management and access to relevant data sources. Communication is an essential element in various operational scenarios and at different levels of the hierarchy of PS organizations. First responders should be able to exchange information (i.e., voice and

data) in a timely manner to coordinate the relief efforts and to improve the situational awareness of the environment.

These capabilities must be provided in a very difficult environment, where critical infrastructures (e.g., energy, communications) are often degraded or destroyed by the natural disaster. Furthermore, natural disasters or emergency crisis are usually unplanned events, which cause panic conditions in the civilian population and affect essential services and resources (e.g., transportation); these conditions make the tasks of first responders even more difficult to achieve. Furthermore, in large natural disasters, many different PS organizations may be involved with different IT and communication systems, which can cause interoperability problems.

The evolution of ICT is associated to concepts like the Internet of Things (IoT) [1], which could be defined as a dynamic global network infrastructure with self configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, which are seamlessly integrated into the information network. In the IoT, "things" are expected to become active participants in business, information and social processes where they are enabled to interact and communicate among themselves and with the environment by exchanging data and information "sensed" about the environment, while reacting autonomously to the "real/physical world" events.

In this context, the concepts of IoT can provide strong benefits to PS organizations by creating a seamless communication framework, which can provide the necessary flexibility to address complex emergency crisis. PS responders are also heavy reliant on the "sensed" information about the environment to create a situational awareness, which improves the decision process and coordination. Pervasive networks could provide ubiquitous access to all the parties involved in a crisis (i.e., civilians and first responders), while new technologies for storing or accessing information could provide more efficient ways to locate necessary data (e.g., building plans) or improve the decision process.

The evolution of ICT to IoT was born in the mainstream or "commercial" domain for civilian use, even if potential applications in PS domain have been mentioned in literature [1]. Therefore, it is important to identify the main challenges and enablers (i.e., technical or organizational), which can foster the adoption of IoT concepts in the PS domain as well.

The deployment of the innovative ICT technologies in the PS domain should be conformant to the operational requirements already defined by PS organizations, which include security, availability, responsiveness, robustness against environmental factors and reliability. A complete description of the PS requirements for PS communications is provided in [2]. Furthermore, PS communication system must provide specific services or functions (e.g., group voice call), which may not have an equivalent in the commercial domain. In this context, this paper will discuss the challenges of the PS domain and the areas where innovative ICT concepts and technological enablers can provide significant benefits.

The rest of this paper has the following structure: Section 2 identifies the current major challenges in the PS domain. Section 3 provides an overview of the current activities by research, industry and government and identifies the enablers and related challenges to deploy IoT concepts and new ICT technologies in the PS domain. The potential evolution scenarios for ICT in Public Safety domain are described in section 4. Finally section 5 concludes the paper.

2. Current ICT Challenges in Public Safety Domain

PS organizations must operate in a difficult environment and in various operational scenarios, which are characterized by a number of significant challenges:

- **Interoperability**. Interoperability barriers among the communication systems of various PS organizations are still present both a national level (among PS organizations of the same region or nation) or among different nations in the same geopolitical area (e.g., Europe). Interoperability barriers are usually based on historical reasons: ICT infrastructures and communication networks were created by each PS organization to address its specific operational requirements. Interoperability barriers in the PS domain are identified by various sources including [3]. In same cases, interoperability barriers are also due to security reasons. In the effort of securing and protecting sensitive data, different cryptography algorithms and cryptography keys are used in networks based on the same technology. Beyond technical issues, interoperability barriers are often more operational than technical. Common procedures and organizational schemes are missing or incomplete to support the coordination of various PS organizations during a national disaster or an emergency crisis. Figure 1 describes the different layers of interoperability.

- **Broadband Connectivity:** Existing or future PS applications are driving the need for broadband connectivity to transmit images or video. The wireless communication technologies currently deployed (e.g., TETRA, APCO25) provide only limited data capacity (e.g., 28.8Kbits). New standards for TETRA and APCO 25 are currently being drafted to support higher data rates, but the deployment of these new technologies may be inhibited by lack of suitable radio frequency spectrum and the limited budget of the involved jurisdictions. A list of potential PS applications, which can drive the need for broadband connectivity, is provided in Table 1.

- **Challenging operational environment:** PS ICT infrastructures may be destroyed or degraded as a consequence of the crisis. For example an earthquake, flooding or tsunami can destroy the physical network infrastructure or disrupt the supply chain used in humanitarian logistics [4]. Even if the ICT infrastructure is not destroyed, it can be overloaded by the increase of traffic due to panic calls as in the London bombing. In some scenarios, PS responders must also operate with limited connectivity or coverage (e.g., underground operations).

- **Equipment lifecycle:** Evolving technologies and standards may cause the existing wireless equipment to become obsolete. The equipment lifecycle in the PS domain is usually less dynamic than the commercial domain. A dedicated PS network and related terminals are usually designed and acquired for a long operational time (e.g., 10-15 years), while commercial networks and terminals may be upgraded every 3-4 years or less. A potential risk is that PS technologies may not follow the technical progress of the commercial domain. This is also the consequence of the different market sizes: there are around 1 billion commercial wireless terminals against 5 millions of PS specific terminals.

The resolution of these challenges will drive the future evolution of ICT in the PS domain.

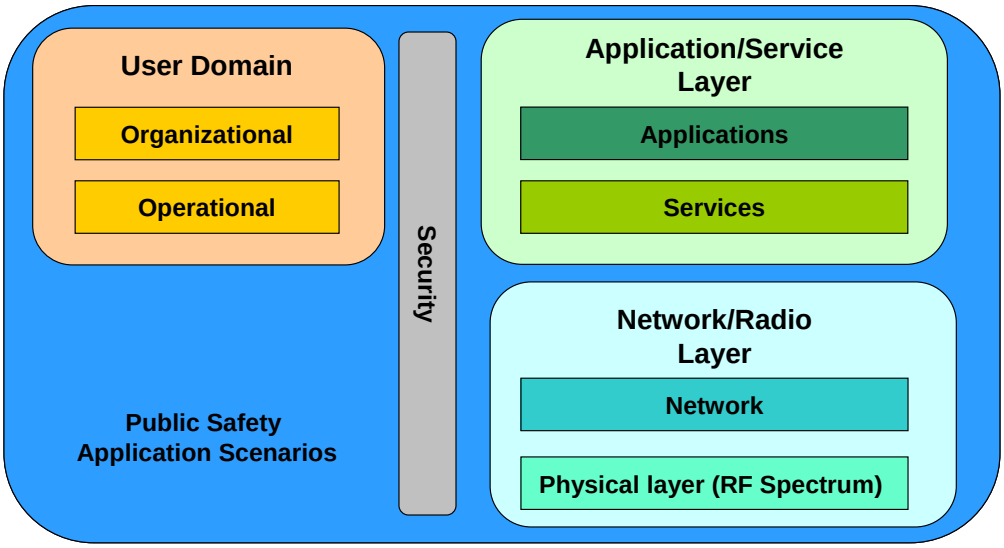

Figure 1. Interoperability Layers

Table 1. Public Safety Applications

Database checks	Public safety officers must often retrieve data from the headquarters to support their work. For example, in a chemical plant fire, public safety officers may need the building plans, the location of specific assets (e.g. water) or the most dangerous areas (e.g. deposit of inflammable liquids).
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 to the headquarters or to a control center to be compared against biometric archives. Then, the response could be sent back to the PS officers. This would be a positive method of identification during field interrogation stops if identification documents (e.g., I.D. card) are missing.
Wireless video surveillance	A fixed or mobile sensor can record and distribute data in video-streaming format, which is then collected and distributed to public safety responders in the area or back to the Headquarters.
Automatic number plate recognition	A camera captures license plates and transmits the image to headquarters to verify that the vehicles have not been stolen or the owner is a crime offender.
Documents scan	During patrolling activities, public safety officers can verify an identification document (e.g. I.D. card or driving license) in a more efficient way. Document scan is also useful in border security operations where people, who cross the borders, may have documents in bad condition or falsified.
Location/Tracking for Automatic Vehicle/Officer Location. Situation Awareness	The public safety officer has a Global Navigation Satellite System GNSS (e.g., GPS) position localizer on the handheld terminal or the vehicular terminal. The positions are sent periodically to the headquarters so that the command center knows the location of the public safety officers and they can organize and execute the operations in a more efficient way.
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 are trapped. Building or floor plans can be requested to the headquarters and transmitted to the public safety responders.
Remote emergency medical service	Through transmission of video and data, medical personnel may intervene or support the rescue team in the field.
Sensor networks	Sensors networks could be deployed in a specific area and transmit images or data to the public safety responders operating in the area or to the command centre at the headquarters. This application does not include video-surveillance, which is previously described.
Monitoring of Public Safety officer	Vital signs of Public Safety officers could be monitored in real-time to verify their health condition. This is particularly important for firefighters and officers involved in search and rescue operations.

3. ICT Enablers in the Public Safety Domain

3.1. Enablers for Broadband Connectivity

The challenge to provide broadband connectivity to Public Safety organizations, has been investigated in [5], which highlighted the fact that, due to the narrowband technologies used in PS communications systems, PS organizations have been limited primarily to voice services and low-speed data transfer on their communication networks. In contrast, current and forthcoming commercial technologies are successfully addressing the provision of broadband services. In this regard, the FCC in USA has submitted the National Broadband Plan (NBP) [6], which advocates a closer collaboration between commercial and PS networks. The NBP addresses the critical issue to ensure the availability of broadband communications for PS and emergency response on a cost-effective and technically feasible basis. One issue is that the allocation of dedicated resources to PS organizations to entirely support the unusual needs during emergencies would leave a great deal of capacity unused between spikes and would be highly inefficient. The FCC white paper "Public Safety Nationwide Interoperable Broadband Network: A New Model for Capacity, Performance and Cost" [7] recommends that PS organizations have access to a new nationwide shared Commercial/PS broadband network to be built over a dedicated 2x5MHz spectrum in 700 MHz band. The sharing of network resources between PS and commercial networks can provide the required broadband capacity in extreme situations and it can adapt to the traffic demands. For example: commercial networks should preserve communications resources to be used by the civilian population to receive information on the status of the emergency, available goods (e.g., medicines) or to contact authorities and relatives. FCC has proposed Long Term Evolution (LTE) as the wireless technology of choice to provide broadband communication and the needed prioritization functions of the communication services.

The sharing concept can be applied to both spectrum and network resources. In Europe, ETSI is currently considering a solution to share part of the spectrum that would be allocated to PS users with other networks under a strict pre-emptive regime that guarantees the recovery of that part of spectrum for mission critical applications [8]. In this case, spectrum sharing can be enabled also with military organizations.

There are a number of organizational and technical challenges, which must be solved to implement and deploy the resource sharing concepts. The challenge is to propose a technology, which is flexible enough to satisfy the operational requirements of the public safety domain (e.g., security, call prioritization) and the business requirements of the commercial domain (e.g., low cost of equipment). Beyond the technical challenges in spectrum sharing, regulatory issues are also of utmost importance. In particular, spectrum regulations can be particularly complex in fragmented geopolitical regions like Europe.

3.2. Enablers for Interoperability

Network sharing also implies significant technical challenges in terms of interoperability and interworking for the integration of PS networks and commercial networks. While, FCC has proposed a new communication network based on LTE technology alone, PS networks are usually "dedicated" networks implemented with various communication technologies and standards (e.g., TETRA, TETRAPOL). They

are also designed and deployed to be used by one or more PS organizations, but not by civilians. As such, they are usually vertical silos with low degree of interoperability even among themselves and far less with commercial networks. Interoperability could be provided through IP gateway or IP based networks, which integrate different Radio Access Technologies (RAT). The new TETRA Inter System Interface (ISI) [9] represents a set of basic services necessary to support cross-border communications among independently owned and operated TETRA networks. The TETRA ISI standard is partially defined [9] and it is still not in operation today. Some companies have faced the first step of ISI certification but the list of functionalities currently tested was limited and it did not include a minimum set of necessary user services. In recent times, the majority of TETRA network suppliers are moving from Time-Division Multiplexing (TDM) to IP based architectures. This suggests that a new ISI standard must be defined based on IP protocols for interconnecting networks providing PS services. The evolution of PS communication networks towards IP would also benefit the integration with future LTE networks. The challenge is to provide the rich set of functionalities needed by PS officers. While basic one-to-one connectivity is relatively easy to achieve, the support for group calls, messaging and broadcast communication can be more complex.

Software Defined Radio (SDR) is another technology, which has been considered to address the interoperability barriers among different wireless communication systems. In ETSI, SDR is defined as "radio in which the radio frequency (RF) operating parameters including, but not limited to, frequency range, modulation type, or output power can be set or altered by software, and/or the technique by which this is achieved". A conventional wireless communication system is designed to transmit in specific frequency bands and the transmission parameters (e.g., modulation) are embedded in the firmware and hardware design. A SDR terminal could theoretically activate software modules to operate in various frequency bands or implement various specific wireless service. Such reconfiguration could be executed when needed: for example during an emergency to connect to an existing wireless network. Wireless services (e.g., UMTS, TETRA) can be implemented in software as "waveforms", which can be executed on the SDR platform. During an emergency crisis, first time responders can use SDR technology and waveforms to interface any needed wireless communication technology present in the area. Beyond mitigating interoperability barriers, SDR technology can also provide additional coverage in the emergency area by adapting the transmission parameter for specific scenario (e.g., underground operations) and extend the coverage of fixed networks.

The SDR could also be used as a relay to provide interoperability among conventional wireless systems. For example, multi-antenna SDR base stations or vehicular SDR terminals can execute two or more waveforms to connect to different RATs and create a "bridge" to transport voice and data originating from terminals based

on different communication standards.

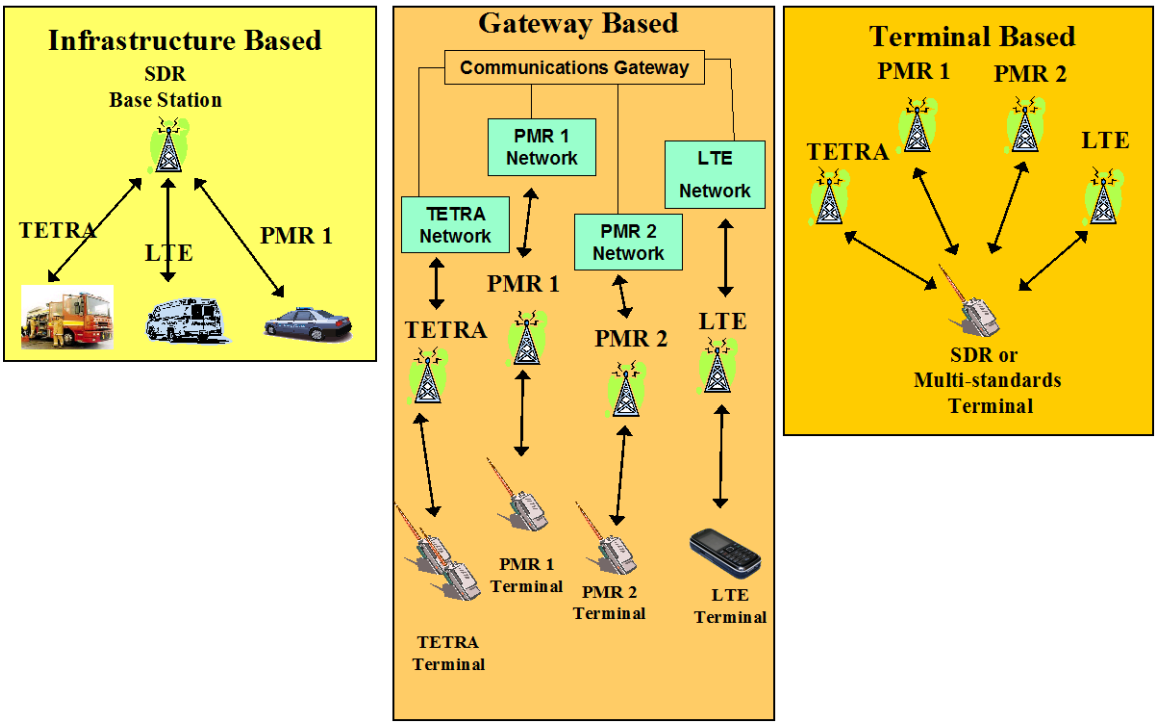

Figure 2 describe the potential use of SDR.

Finally, the reconfigurability offered by SDR can also mitigate the challenge of the equipment lifecycle and upgradeability described in Section 2. A large PS national or regional network is usually a huge economic investment for 10-15 years or more. The evolution of a PS communication network based on SDR technology can be mostly achieved through software upgrades, which is considerably less expensive than hardware upgrades. The upgradeability provided by SDR technology can also significantly increase the lifetime of PS networks and enable a faster evolution of the communication equipment.

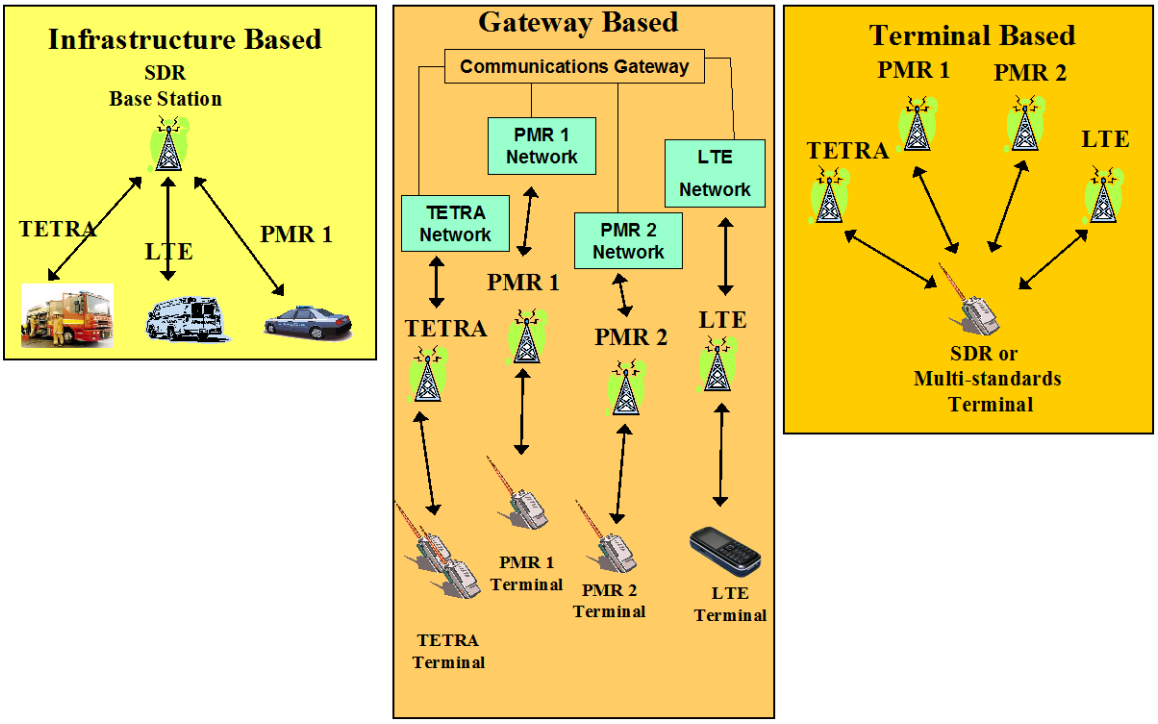

Figure 2. Potential Use of SDR to Address Interoperability Barriers

While SDR technology, and/or IP gateways and standard inter-system interfaces can mitigate the interoperability barriers at the physical and network level, PS organizations may still not be interoperable at the upper layers of the ICT infrastructure (i.e., information, services and applications). To enable interoperability over all layers of a communication system, new approaches for information and data exchange must be investigated and identified for the future development of ICT in the PS domain. This subject will be discussed in the following Section 3.3.

3.3. Enablers for Information Management

To underline the benefits of interoperability on the information level, a new type of Crisis Information Management System (CIMS) is in the focus of research [10]. These types of systems should run in parallel with existing systems to aggregate all information and bundle them at least in one single office or authority. The authority is not necessary a superior authority, but can also act as a coordination and information sharing point.

The CIMS and the corresponding framework provide key top-level functional services:

- Incident Management
- People Management
- Resource Management
- Notification Management
- Situation Awareness Management

It can be shown that the aggregation of different sources of information into a system will lead to positive effects for the whole disaster management process. Nevertheless, a complete data model or markup language is required in order to enable the exchange of information between all parties concerned, which will be discussed in the following paragraphs. In most PS applications, the data (e.g., image) should not only be collected but it should also be enriched with context information (e.g., scenario, source organization). To support this functionality, a semantic layer has to be added to combine the collected data into ontology-based context models.

To compete with the challenges of information sharing, the development of the EDXL (Emergency Data Exchange Language) suite of standards started. The goal of this standardization process is to enable a seamless data sharing across jurisdictions and different departments [11]. To make a market entrance possible, various research projects focused on a simplification of the described EDXL based process. The use of a middleware should help to improve interoperability between existing systems over the boundaries of various jurisdictions and technologies. The major goal of all projects is to research new concepts for scaleable systems and protocols, which could be used in daily operations as well as in spare and complex disaster scenarios.

The vision behind the Unified Incident Command and Decision Support (UICDS) System is the interconnection of all users through open and standardized interfaces. The information sharing is role based and information specific, which means that the UICDS-Core (UCore) should distill the given information into EDXL-coded elements needed in specific emergency scenarios. To prevent an encapsulation of different systems because of data-security or privacy aspects, all of the information is split up into fractional data. These pieces of data represent the smallest possible unit of shareable information, which can be freely shared within the network in digest form (recipient specific combination). Though the UICDS includes novel ideas on the way to comprehensive interoperability, the complexity prevents the actual use in real systems because of the high effort to interconnect existing systems to the UICDS.

In Europe, a novel solution is presented as a result of the research project SPIDER [12]. As the core of a federation of systems, a new Protection and Rescue Markup Language (PRML) was designed for efficient information sharing. The use of characteristic principles of a Service-Oriented Approach (SOA) lead to an open system of systems, in which every organization is enabled to preserve their own software applications and data and be interoperable with other organizations and systems.

The federation of systems, defined in SPIDER project has the following features:

- An Open Architecture and standards-based
- Modular and scalable
- Flexible to fit a various spectrum of use-cases
- Focusing on security and privacy by design.

The standardization of different interfaces and access rules is a key activity. The objective is to enable a loose coupling of systems, operated by each of the involved organizations for a specific purpose. The standardization should define of all necessary elements of the communication process, including entity descriptions, data models, roles and permissions.

A generic description of the communication architecture is depicted in Figure 3. Two major components are defined as the basis of the model: Agent and Entity. It should be pointed out that in both components a subset of the features is mandatory and another

subset is optional to obtain a greater flexibility. The mandatory features are part of the standardization, because they build the minimal core functionality of the proposed System of Systems. The Agent describes a set of mandatory and optional services. The set of mandatory services includes all services needed to fulfill a specific role. The Entity is an information provider in the system, which is basically a set of Agents. It represents an organization and has to fulfill the requirement, which all information have to be included in the descriptions which are necessary for the set-up of an interconnection.

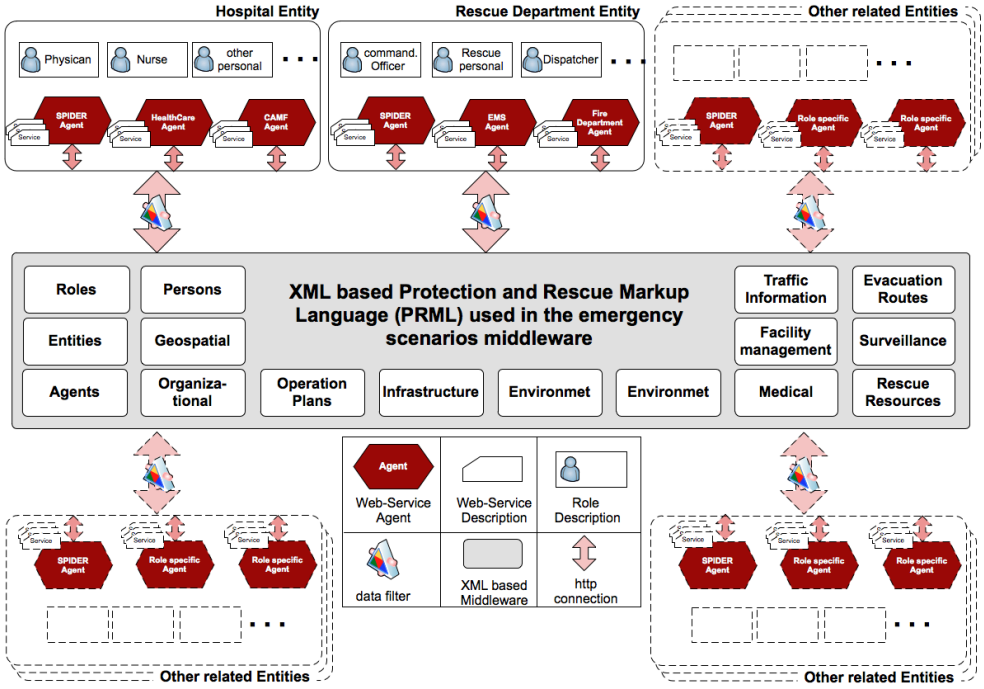

Figure 3. Federation System Architecture

To ensure the integration with IoT technologies and concepts, all interconnections developed in the project are based upon well established internet standards. The core protocols are web services for the communication and XML as information carrier.

This approach is independent of its underlying technologies. The inclusion of all information into the middleware (i.e., systems' description, protocols, data) enables a holistic design of a system of heterogeneous systems. With the possibility of modeling roles and procedures as well as filter for information, an autonomous federation engine is placed to support the human operators of such systems to get access to the right data, at the right time within the right visualization. In conclusion, this approach provides interoperability among the applications and services of different organizations.

4. Evolution paths for ICT in the Public Safety domain

The adoption of new ICT technologies in the PS domain is not driven by business factors as in the commercial domain but it is also based on political support to PS organizations, budget availability, public attention to the protection and security of the citizens, increased risks of intentional or unintentional threats (e.g., terrorist attacks)

government sensitivity to the adoption of new technologies and so on. All these forces will drive the adoption and evolution of new technologies.

We can identify three different roadmaps for the evolution of ICT in the Public Safety domain (see [13]):

- *Slow incremental growth*. In this scenario, 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 PS sector is limited. Voice communications remains dominant. There is lack of political support for cross-border interoperability among PS organizations of different nations. PS network and commercial networks are not integrated and they are not interoperable. Availability of broadband connectivity is hampered by lack of allocated spectrum bands. Command centers and their users and applications are not interconnected.
- *Information driven growth*. In this scenario, 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 PS officers in the field and among the control centers. 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. Spectrum bands are made available to support wideband communication but not broadband communications. There is a limited integration among commercial and PS networks like interoperability at the application layer, simple connectivity for voice and data (e.g., no group calls) or distributed messaging. Specific applications and functions of command centers are interconnected and integrated but no common standards and frameworks are defined. Security and privacy issues are not fully addressed, beyond basic functions (e.g., authentication).
- *Full multimedia and convergent networks*. In this scenario, 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 PS networks. PS officers are used to conduct their operation on the basis of broadband applications like common operational picture. Interoperability barriers are mitigated through various technologies (e.g., SDR, SOA). 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. Command centers are fully interconnected and integrated. Applications are seamlessly interoperable but sensitive data is protected from unauthorized users. Standards for federated systems are defined and implemented.

5. Conclusions

This paper presented the most critical challenges for the evolution of ICT technologies in the PS domain. Various potential technologies have been identified and described. Figure 4

describes how the various technologies can address the challenges at different layers of the ICT infrastructures.

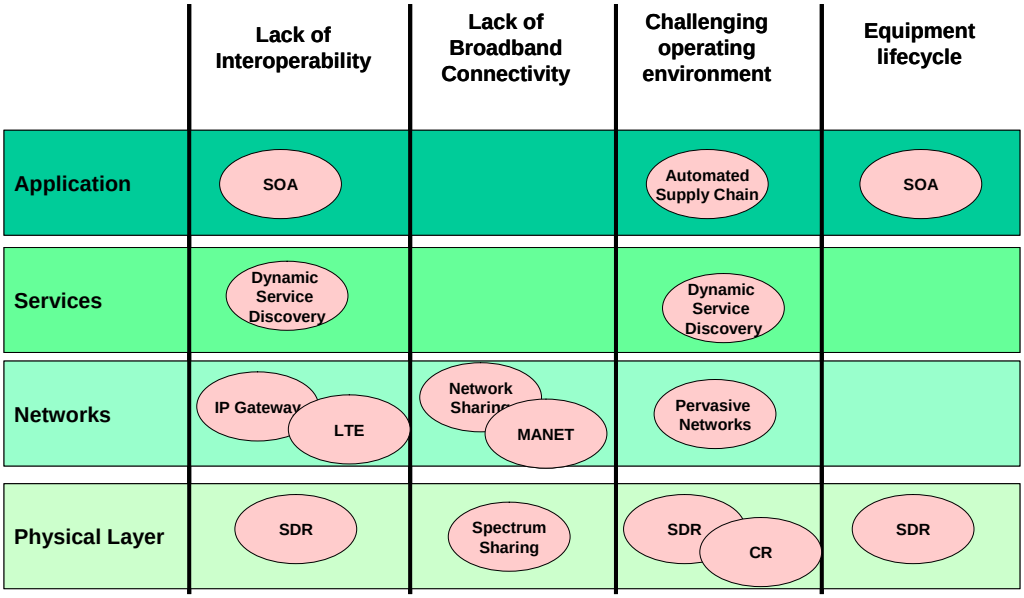

Figure 4. Challenges and Related Technologies

As described in Section 4, the evolution of ICT in the Public Safety domain is dependent on many causes including political, business and regulatory factors. One of the main factors is that public safety is considered a niche market. It is certainly true that PS market is three orders of magnitude smaller than the commercial market. On the other side of the coin, all the emergency crisis occurred in the last years (including terrorist attacks) have highlighted the importance of providing effective ICT enablers to the vast number of public safety officers involved in disaster management all over the world.

References

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey", Computer Networks, Volume 54, Issue 15, 28 October 2010, pp. 2787-2805.

[2] SAFECOM, US communications program of the Department of Homeland Security. "PS Statements of Requirements for communications and interoperability v I and II".

[3] V. Mayer-Schonberger, "The politics of public safety communication interoperability regulation", Telecommunications Policy, Volume 29, Issue 11, Network Security, Survivability and Surveillance, December 2005, Pages 831-842.

[4] B. Balcik, B. M. Beamon, C. C. Krejci, K. M. Muramatsu and M. Ramirez, "Coordination in humanitarian relief chains: Practices,challenges and opportunities", International Journal of Production Economics, Vol. 126, No. 1, 2009, pp. 22-34.

[5] J.M. Peha, "Regulatory and policy issues protecting PS with better communications systems", IEEE Communications Magazine, vol.43, no.3, March 2005, pp. 10- 11.

[6] Federal Communications Commission. National Broadband Plan, March 2010.

[7] The Public Safety Nationwide Interoperable Broadband Network: A New Model for Capacity, Performance and Cost. FCC White Paper, June 2010.

[8] ETSI TR 102 628 V1.0, "System reference document; Land Mobile Service; Additional spectrum requirements for future Public Safety and Security (PSS) wireless communication systems in the UHF frequency range (300 MHz to 790 MHz)", March 2005.

[9] ETSI TR 101 448 V1.1.1, Terrestrial Trunked Radio (TETRA); Functional requirements for the TETRA ISI derived from Three-Country Pilot Scenarios, 2005.

[10] R. Iannella and K. Henricksen, "Managing Information in the Disaster Coordination Centre: lessons and opportunities", in ISCRAM 2007 Conference, Delft, The Netherlands, May 2007.

[11] D. Gusty and S. Dwarkanath, "Improving the Effectiveness of Emergency Response through Improved Standards", in Proceedings of the 11th Annual international Digital Government Research Conference on Public Administration online: Challenges and Opportunities, Puebla, Mexico, May 17- 20, 2010.

[12] S. Subik, S. Rohde, T. Weber and C. Wietfeld, "SPIDER: Enabling interoperable information sharing between public institutions for efficient disaster recovery and response", IEEE International Conference on Technologies for Homeland Security (HST), 8-10 Nov. 2010, pp. 190-196.

[13] ETSI TR 103 064 V1.1.1 (2011-04), "Reconfigurable Radio Systems (RRS); Business and Cost considerations of Software Defined Radio (SDR) and Cognitive Radio (CR) in the Public Safety domain", April 2011.

Authors

Gianmarco Baldini completed his degree in 1993 in Electronic Engineering from the University of Rome "La Sapienza". He has worked in management positions in multinational companies like Ericsson, Alcatel-Lucent, Hughes Network Systems and Finmeccanica before joining the Joint Research Centre of the European Commission in 2007 as Scientific Officer. He has published more than 30 papers in international journals and conferences. His current research activities focus on communication services for PS and security aspects in GNSS services.

Oriol Sallent is Associate Professor at the Universitat Politècnica de Catalunya. His research interests are in the field of mobile communication systems, especially radio resource and spectrum management for cognitive heterogeneous wireless networks. He has published more than 150 papers in international journals and conferences. He has participated in several research projects of the 5th 6th and 7th Framework Programme of the European Commission and served as a consultant for a number of private companies.

Sebastian Subik received his Diploma in Information Technology from TU Dortmund University in 2007. Since then, he is working as a Research Assistant at the Communication Networks Institute (CNI), TU Dortmund University. At the CNI, he is involved with the Emergency Response Management and Wireless Robotics Research Group. His main research interests are emergency communication networks with a focus on enhancing the operational and TETRA.

After **Christian Wietfeld** has completed his PhD in Wireless Network Engineering at RWTH Aachen University in 1997, he held the position of a Director System Engineering / Product Line Management at Siemens Communication. He joined the Faculty of Electrical Engineering and Information Technology of TU Dortmund University in April 2005 to head the Communication Networks Institute (CNI). Since 2010, he also holds the position of the Dean of the Faculty. His research work on the design and performance evaluation of communication architectures, protocols and services has been published more than 150 conference papers, book chapters, contributions to standardization (ITU-T/3GPP/ETSI/OMA) and patents.