

FP7-285556 SafeCity Project



Deliverable D2.7

Public Safety Scenarios guidelines and conclusions

Deliverable Type: CO

Nature of the Deliverable: O

Date: 27/10/2011

Distribution: WP1

Editors: ISD

Contributors: ISDEFE

***Deliverable Type:** PU= Public, RE= Restricted to a group specified by the Consortium, PP= Restricted to other program participants (including the Commission services), CO= Confidential, only for members of the Consortium (including the Commission services)

**** Nature of the Deliverable:** P= Prototype, R= Report, S= Specification, T= Tool, O= Other

Abstract: This document provides concrete guidelines and methodology to carry out successfully the scenarios characterization, it provides a summary of the key point found along the 6 cities characterization. Also it summarizes the workshop methodology and the conclusions arise during the event.

DISCLAIMER

The work associated with this report has been carried out in accordance with the highest technical standards and SafeCity partners have endeavoured to achieve the degree of accuracy and reliability appropriate to the work in question. However since the partners have no control over the use to which the information contained within the report is to be put by any other party, any other such party shall be deemed to have satisfied itself as to the suitability and reliability of the information in relation to any particular use, purpose or application.

Under no circumstances will any of the partners, their servants, employees or agents accept any liability whatsoever arising out of any error or inaccuracy contained in this report (or any further consolidation, summary, publication or dissemination of the information contained within this report) and/or the connected work and disclaim all liability for any loss, damage, expenses, claims or infringement of third party rights.

List of Authors

| Partner | Authors |
|---------|---|
| ISDEFE | Diego Giménez, Judith Pertejo, Pilar Campos |

Document History

| Date | Version | Editor | Change | Status |
|----------|---------|--|---|--|
| 20110901 | 0.1 | Judith Pertejo and Diego Giménez | Skeleton and first inputs | First incomplete draft |
| 20110930 | 0.3 | Diego Giménez, Judith Pertejo and Pilar Campos | WS report | First complete draft |
| 20111021 | 0.6 | Diego Giménez, Judith Pertejo and Pilar Campos | Conclusions and general overview | Final version with pending internal review |
| 20111027 | 0.7 | Diego Giménez, Judith Pertejo and Pilar Campos | Final corrections based on internal reviewers' comments | Final version |

Table of Contents

| | |
|--|------|
| List of Authors | iii |
| Document History | iv |
| Table of Contents | v |
| List of Figures | vii |
| List of Tables..... | viii |
| Glossary..... | ix |
| References..... | x |
| 1. Introduction..... | 1 |
| 1.1 Purpose of this document..... | 1 |
| 1.2 Scope of this document | 1 |
| 2. General guidelines for Public Safety Characterization | 3 |
| 3. Workshop | 5 |
| 3.1 Workshop objective..... | 5 |
| 3.2 Workshop methodology | 6 |
| 3.2.1 Preparation for the WS..... | 7 |
| 3.2.2 During the Workshop | 9 |
| 3.2.3 After the Workshop..... | 9 |
| 3.3 Workshop Content..... | 9 |
| 3.4 Workshop Conclusions | 16 |
| 3.4.1 General overview | 16 |
| 3.4.2 End-Users Requirements..... | 16 |
| 4. Key conclusions of European Public Safety Systems | 39 |
| 4.1 PS Characterization in EU cities | 39 |
| 4.1.1 Situational Awareness area | 39 |
| 4.1.2 Command Centre Area | 41 |
| 4.1.3 Alerting Citizens area..... | 41 |
| 4.1.4 Ad-hoc Networks area..... | 42 |
| 4.2 Social, ethical and legal considerations | 42 |
| 4.3 Challenges arisen from User Requirements | 45 |
| 5. Annexes | 49 |
| 5.1 Annex 1 – Public Safety Scenarios Template | 49 |
| 5.2 Annex 2 – End user Questionnaire Template | 50 |

5.3 Annex 3 – Workshop Agenda..... 51

5.4 Annex 4 – Attendees List 53

5.5 Annex 5 – Invitation Letter 55

List of Figures

Figure 1 Task 2.1 schedule 4

Figure 2 Worshop Methodology I 6

Figure 3 WS Methodology II 7

Figure 4 MCC: CISEM & CISEVI – WS 10

Figure 5 Bucharest BTMS system - WS..... 10

Figure 6 Athens SYZEFXIS - WS..... 11

Figure 7 Stockholm Public Safety and C2 - WS..... 12

Figure 8 Helsinki Police and CCTV system - WS..... 13

Figure 9 Obidus Actual Public Safety - WS 14

Figure 10 SafeCity architecture 15

Figure 11 SafeCity applications 15

Figure 12 Share on-line services..... 32



List of Tables

| | |
|--|----|
| Table 1 Public Safety and Security entities involved in User Requirements collection..... | 8 |
| Table 2 Intelligence surveillance - Users Requirements..... | 18 |
| Table 3 Citizens abnormal behavior detection - Users Requirements | 19 |
| Table 4 Security – Objects detection - Users Requirements | 20 |
| Table 5 Safety – Environmental Surveillance - Users Requirements..... | 21 |
| Table 6 Safety – Traffic surveillance - Users Requirements | 23 |
| Table 7 QoS for surveillance systems - Users Requirements | 24 |
| Table 8 Connectivity and integration in Surveillance Systems - Users Requirements | 25 |
| Table 9 Sensitive data constrains - Users Requirements | 26 |
| Table 10 Command and Control Centre - Users Requirements | 27 |
| Table 11 Alarms management - Users Requirements..... | 28 |
| Table 12 Surveillance Equipment management - Users Requirements | 29 |
| Table 13 Visualization - Users Requirements | 30 |
| Table 14 Networks management - Users Requirements | 31 |
| Table 15 Shared on line services- Surveillance integration - Users Requirements | 33 |
| Table 16 Shared on-line services- Unified Emergency response activities - Users Requirements | 34 |
| Table 17 On-line services for deployed units - Users Requirements..... | 35 |
| Table 18 Security management - Users Requirements..... | 36 |
| Table 19 Alerting citizens - Users Requirements..... | 37 |
| Table 20 Ad-hoc Network - Users Requirements | 38 |
| Table 21 Regulations and Laws | 43 |
| Table 22 Requirements from Social, ethical and legal considerations..... | 44 |

Glossary

| Acronym | Meaning |
|---------|--|
| C2 | Command and Control |
| CCTV | Close Circuit TV |
| CISEM | Integrated Security and Emergency Center of Madrid |
| CISEVI | Integrated Video Systems |
| EU | European Commission |
| FR | First Responder |
| GIS | Geographic Information System |
| GPS | Global Positioning System |
| ICT | Information & Communications technology |
| IP | Internet Protocol |
| IT | Information Technology |
| LTE | Long Term Evolution |
| MCC | Madrid City Council |
| PMR | Private Mobile Radio |
| SMS | Short Message System |
| TETRA | Terrestrial Trunked Radio |
| WS | Workshop |

References

| Number | Reference |
|--------|---|
| [1] | D2.1 Madrid Public Safety Scenario |
| [2] | D2.2 Bucharest Public Safety Scenario |
| [3] | D2.3 Athens Public Safety Scenario |
| [4] | D2.4 Stockholm Public Safety Scenario |
| [5] | D2.5 Helsinki Public Safety Scenario |
| [6] | D2.6 Obidus Public Safety Scenario |
| [7] | Internal repository with Workshop Slides presented <i>Meetings/13 - Final User 1st Workshop 20110906/Slides</i> |

1.Introduction

1.1 Purpose of this document

The present document the leadership of Task 2.1 *Public Safety Scenarios*, which has two clear objectives:

- To identify current situation of EU Cities, in terms of ICT in Public Safety area.
- To identify needs that advanced Internet-based networks would potentially satisfy.

Present report D2.7 aims at synthetizing the main issues originated under each city analysis and collecting Public Safety and Security needs that will potentially drive the following steps to be taken in the project. Therefore, it takes the leadership of the global task (T2.1 *Public Safety Scenarios*) providing the main outcomes of the analysis of end users' needs

In order to comply with these objectives the present document counts on six European Cities analysis (Madrid, Bucharest, Athens, Stockholm, Helsinki and Óbidos) performed under subtasks 2.1.1-2.1.6. Present deliverable D2.7 sets common guidelines and methodology to be followed and summarizes the main outcomes arisen from cities' analysis. This procedure facilitates the unification and homogenization of the work and allows D2.7 to concentrate the interaction interface of T2.1 with other tasks within the project. In addition, the organization of a workshop is envisaged in order to support this activity and force the proper collection of end-user requirements.

1.2 Scope of this document

In order to identify current situation of EU Cities in terms of ICT in Public Safety area, D2.7 specifies concrete points to be covered in the cities' deliverables [Sec2tion]. Cities subtask leaders should perform an ad-hoc and detailed analysis of each city context that derives in an innovative simple scheme proposition of Public Safety enhancement in each of them. Within this analysis it is included the status of these cities' ICT infrastructure currently deployed, relevant capabilities currently available, limitations and gaps of current systems, on-going initiatives and future necessities, among others. All this information will help to identify critical needs that advanced Internet-based networks would potentially satisfy in the Public Safety field. Special attention is paid on applications that SafeCity will later implement. This analysis has been possible thanks to on the close collaboration of Public administration entities in charge of Public Safety Services of these six EU cities, in certain cases with direct involvement of SafeCity partners, and in others, being part of the end-users Advisory Board therefore acting as external advisory.

Present document also includes the Scenarios Workshop report [Section3] indicating the steps to be performed within the preparation, over the course of the WS and afterwards. Major conclusions arisen from this event comprise a wide set of user requirements lists. These requirements allow the technical research to incorporate user views regarding functionalities and potential capacities into enablers analysis. WS outcomes are also taken into consideration by cities deliverables (D2.1-6) in order to complement the research of all several aspect aspects under analysis (current systems, operation procedures, capabilities, infrastructures, normative).

The main results and conclusions of the overall research are collected in [Section4]. It summarizes the main ICT systems and outcomes of cities analysis. It includes the ethical policies and regulations of each Member State which will serve as baseline for the complete analysis on T7.1 Social, ethical and legal implications. User needs and functionalities still to be covered and potential challenges included as part of this conclusion section will especially help in the definition of SafeCity enablers of T2.2 *Enablers definition*.

2. General guidelines for Public Safety Characterization

Task 2.1 is composed of 6 subtasks corresponding to analysis of the 6 cities scenarios and a horizontal task that aims at homogenizing the research activities performed in the rest of subtasks. The definition of each scenario is carried out following a common template [Annex 1 – Public Safety Scenarios Template] which presents concrete guidelines to be covered within the study.

The objective of this task is to characterize for each city the current state of the art of the key systems that enable Public Safety capabilities, to finally depict future capabilities to be included in order to enhance the systems currently in use but also to give an overview of the main characteristics of the cities which are of interest for the scope of the project. The work performed along this task will be used as a basis for the future advancement of SafeCity project since it will provide an extensive overview of Public Safety in European cities.

The study starts giving a deep description of the city, including general information as population, events, religion, crime rate, etc. but also listing the main infrastructures available in the city, covering from critical infrastructures and facilities (transportation, railways, etc.) to communication infrastructures, both Public ICT infrastructures, which provides network connection to the general public, and Private ICT infrastructures, which are managed and controlled by local authorities or Public safety agencies.

Moreover, the study includes *“Public Safety Characterization”* which defines the current state of the art of the key systems in terms of Public Safety. The characterization is classified into different functionalities areas: Citizen behaviour, road track incident management, environmental monitoring, alerting citizens and ad-hoc network. In order to follow a common path among the different cities' characterization processes, the definition starts identifying the applications and giving then further explanation, including: components and infrastructure deployed, system architecture involved in the application, requirements, etc. In addition, actuation procedures and methodologies that Public Safety agencies deploy while interacting with them have to be included.

Additional issues have to be analysed to depict the future characterization, in particular related to the analysis of gaps of the applications currently in use, problems usually detected by end users and technological constraints in the current applications; on-going initiatives showing current approaches undertaken by administration or Public Safety agencies and possible ideas for the future are also investigated.

The figure below shows the schedule followed to complete the research within the task 2.1.

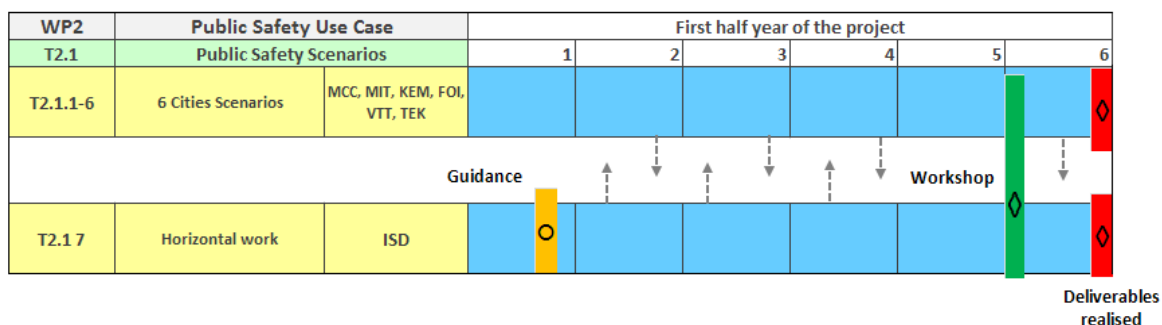


Figure 1 Task 2.1 schedule

The common template is provided to the partners in M1 by leader of D2.7. Along the task duration, persistent contacts are carried out in order to obtain a common and organized work, getting inputs from the rest of the sub-tasks. The scenarios workshop takes place at the beginning of M6 generating new inputs for each city, the methodology to follow for the Workshop development is further explain within [Section3].

The final version of each document should be delivered by the end of M6

3. Workshop

A Scenarios WS took place in Madrid on 6th September at ISDEFE premises. Most of the members of the Advisory Board and two partners directly involved as part of SafeCity Consortium were present with the role of being end users.

Madrid City Council through its Security Division responsible among other issues of providing the technological tools and means for Madrid Police Department labour. On behalf of MCC the attendees were the following: Fernando Garcia, Head of Innovation Department Unit; Sara Gutierrez, Unit Chief of Innovation at the Innovation Department; Javier F Martínez; Carlos Rubio; Gerardo Alonso, Rafael de la Gándara and Ernesto Gómez.

The **Centre for Security Studies Kemea** is a scientific, consulting and research agency, whose purpose is to conduct theoretical and applied research and to produce studies, particularly at a strategic level, on issues concerning security policies. KEMEA also provides advisory and consulting services to the Ministry of Public Order and other authorities on these same issues. Giorgios Eftychidis was the representative.

Bucharest Mayor Office Sector 2 was represented by Valentin Ifrim, Director of the IT and Equipment Administration Directorate within Bucharest Mayor Office Sector 2.

Greneva Civil Protection from Greece was represented by Giorgos Dourelas.

Representing **Attunda Fire Department**, fire department in Stockholm, was Rickard Westning .

From Helsinki, there were representatives from different Public Safety agencies **Helsinki City Council** represented by Anssi Lehtinen, Chief of Preparedness City of Helsinki Mayors Office, and **Helsinki Police Department represented** by Jussi Doivisto, Helsinki Police Department Operational Policing Unit.

The Attendees list is showed in [Annex 4 – Attendees List] in detail listing end users and other workshop attendees on behalf of SafeCity consortium.

3.1 Workshop objective

The objectives of the workshop are to discuss and agree about the systems already existing and needs or functionalities not cover yet. These inputs will be used as support to the activities previously carried out during the scenarios characterization, helping to the elaboration of the analysis and evaluation of specific situation in the cities where SafeCity concept is fully present.

3.2 Workshop methodology

The methodology to be followed to better reach the objectives emphasizes the active contact with end users during and even previously to the workshop. The methodology could be divided into three different steps:

- Preparation for the workshop
- During the workshop
- After the workshop

Below it is shown the methodology proposed to be followed for the Workshop:

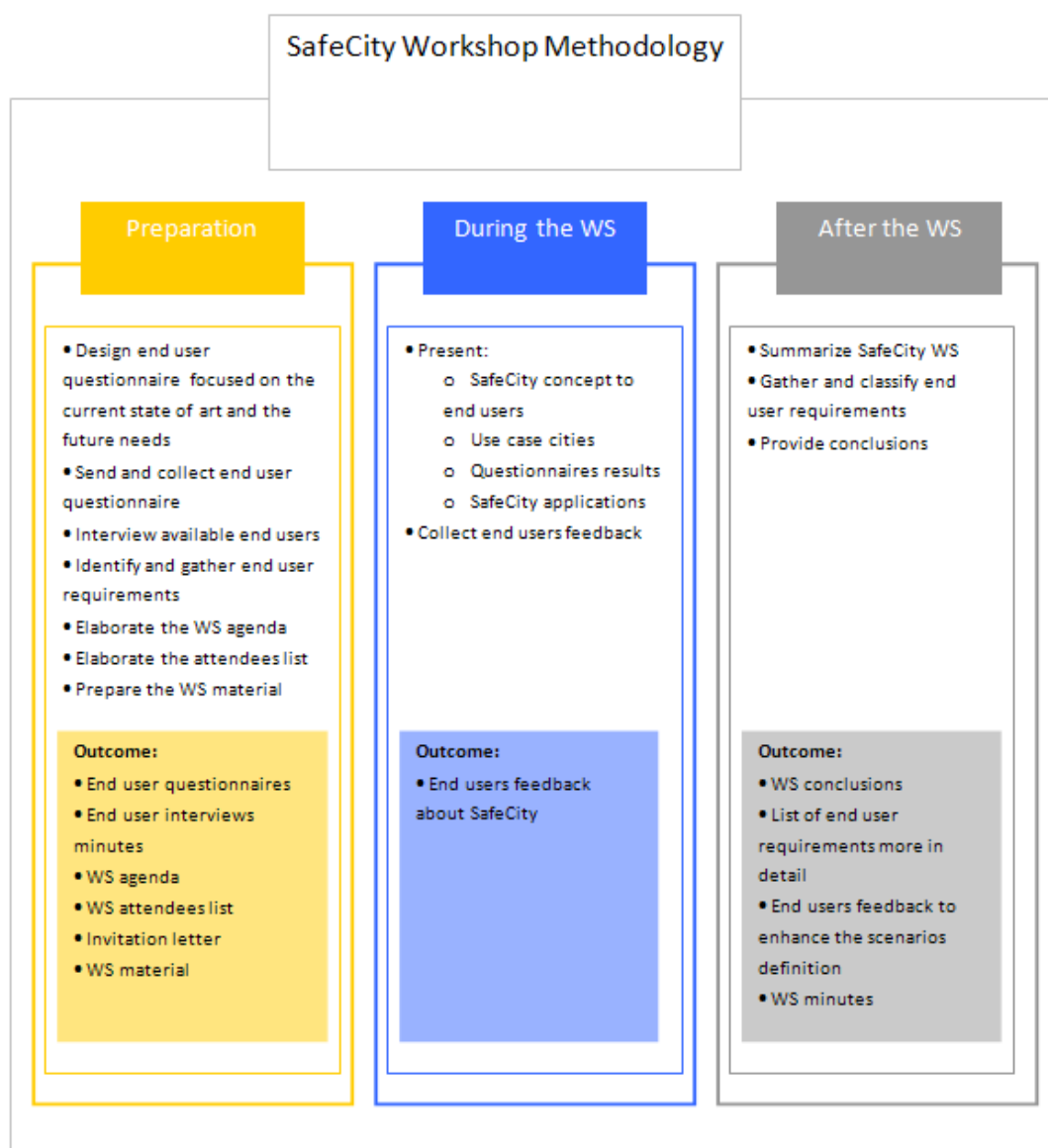


Figure 2 Workshop Methodology I

The figure below shows the timeline of the workshop development, going through the different phases, explained in the detail in the following sections. The general idea is making a real important effort in advance to the WS in order to initiate and foster discussion among the end users and technical analysts during the event and therefore, obtain fruitful outcomes and conclusions.

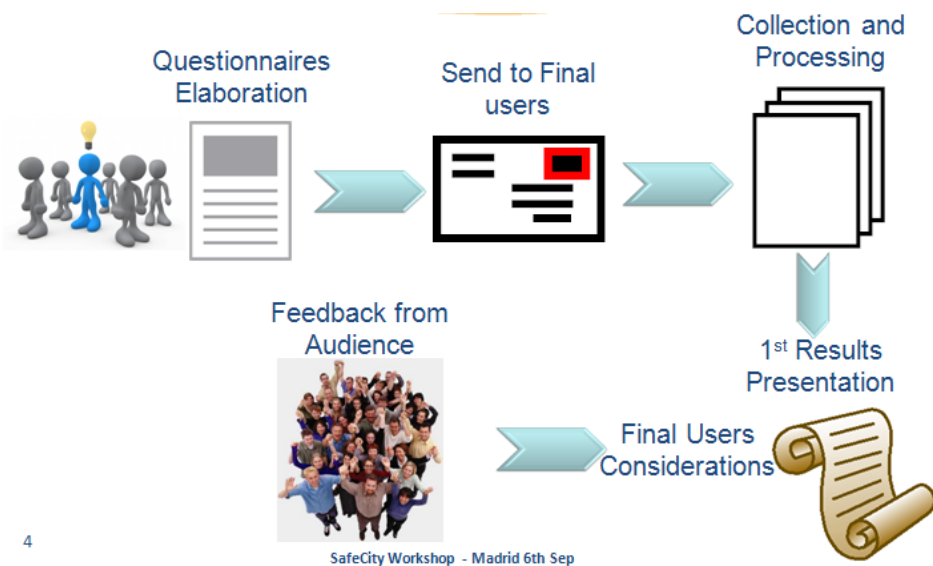


Figure 3 WS Methodology II

3.2.1 Preparation for the WS

The first step is to elaborate an end user questionnaire [

Annex 2 – End user Questionnaire Template] to gather information about the current state of art of the technologies and applications used by end users, their working procedures and their future needs. Apart from this, carry out interviews with available end users since the information gathering is more efficient. A first approach of users' requirements and needs are identified from this information.

Once this information is collected, the WS agenda [Annex 3 – Workshop Agenda] is elaborated considering the WS main objective which involves identifying the end user's needs, in order to complete the requirements already gathered with the questionnaires information, and determine how to cover it using applications based on the Future Internet.

Besides a list of attendees [Annex 4 – Attendees List] is made, taking into account the potential end users and the project partners and after that an invitation letter [Annex 5 – Invitation Letter] is distributed among the attendees.

Finally, WS presentations are prepared by the consortium and the end users in charge of use cases according to the agenda.

As indicated, data collection from this group is expected via questionnaires/surveys related to both systems already existing and needs/functionalities not covered. In addition personal and individual interviews with end-users belonging to the Experts Committee will be performed if required.

The following table shows the different end-users; from them the requirements have been collected:

| #Ref | State | Public Safety and Security Entity |
|-------|----------|--|
| Ref 1 | Greece | Civil Protection Department of Regional Section of Grevena, Athens |
| Ref 2 | Greece | Public security services in the city of Athens: <ul style="list-style-type: none"> • Hellenic Police and Traffic Police Division, • Civil Protection, Fire Brigades, Emergency services (Ambulances) and Hellenic Coast Guard. |
| Ref 3 | Romania | IT Systems and Equipment Administration of Bucharest Municipality Sector 2 |
| Ref 4 | Spain | Command Centre of Madrid M30 Tunnel |
| Ref 5 | Spain | Innovation department and ICT department of Madrid City Police |
| Ref 6 | Sweden | Attunda Fire Department in Stockholm |
| Ref 7 | Finland | Administration Centre in City of Helsinki |
| Ref 8 | Portugal | Óbidos Municipality |

Table 1 Public Safety and Security entities involved in User Requirements collection

3.2.2 During the Workshop

The Scenarios Workshop was held in Madrid (6th September 2011) and was hosted by ISDEFE.

The purpose of this Workshop is to force discussion over existing capabilities in Public Safety area throughout Europe and to identify critical gaps and future innovative applications that may be potentially solved by the Future Internet. The following activities take place:

- SafeCity scenarios and applications: presentation to the audience the cities that has been considered and the 8 applications that will be developed along the project
- Results of end-users questionnaires: a summary of Public Safety and Security requirements collected from questionnaires sent to the final users.
- Feedback from end-users on SafeCity features.

3.2.3 After the Workshop

All the scenarios and applications are presented to the workshop attendees for discussion, in order to collect operational and technology advice, allowing the consortium, in particular each scenario and technological partners, to incorporate end-users and external point of view to the current analysis.

Each city leader, within each own deliverable, incorporate a detail analysis and synthesis of the workshop results, enhancing the existing aspects (current systems, operation procedures, capabilities, infrastructures, normative) and the scenario definition.

3.3 Workshop Content

Firstly, a general overview of SafeCity project was presented where it was commented the importance of enhancing Public Safety in Europe considered important from the point of view of several layers Social, Political and Technical. It was explained briefly the SafeCity framework and concept, focussing on 4 functional areas Situational Awareness, Command Centres, Alerting Citizens and Ad-hoc Networks. Finally, the main outcomes provided by SafeCity to enhance Public Safety in European cities were indicated: Innovative Internet-based capabilities/applications; a set of technical, functional and non-functional specifications; set of enablers and the development of 8 Public Safety applications

After that, the use cases cities were presented:

- Madrid (Spain). Presented by Ms Sara Gutiérrez. She mainly talked about CISEM (the Integrated Madrid City Council Security and Emergencies Centres) and CISEVI (Centralized Video System). Regarding CISEM, she explained which first responders were integrated in CISEM, how centres CISEM was made up, what integrated systems for security and emergencies had and what communications technologies used; and regarding CISEVI, she explained the structure and how it was used.

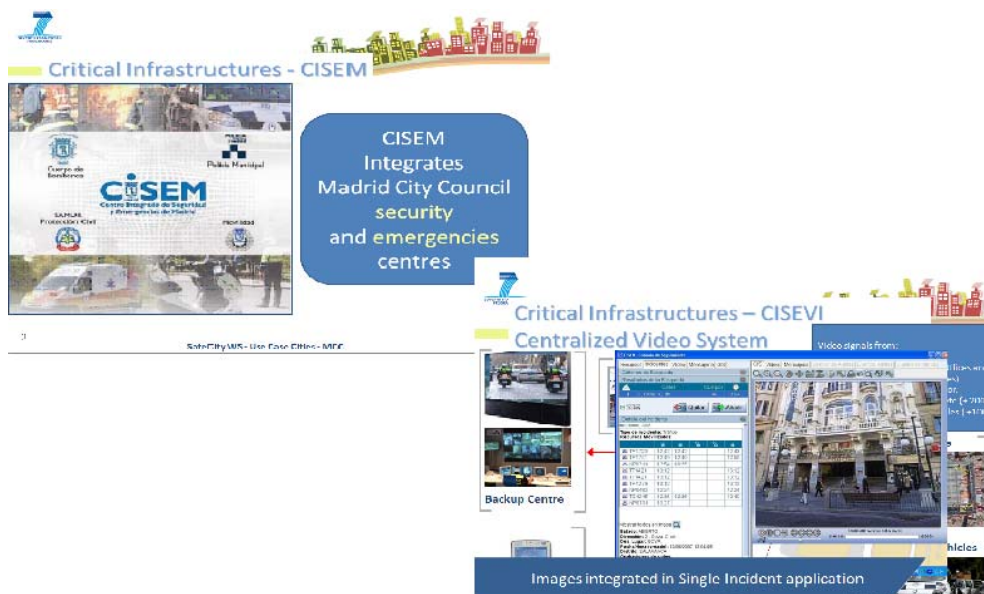


Figure 4 MCC: CISEM & CISEVI – WS

- Bucharest (Romania). Presented by Valentin Ifrim, and Adrian Sima, Mira Telecom. They showed a high overview of the city and highlight the Bucharest Traffic Management System (BTMS). Its explanation included main features, basic and advanced functionalities as the benefits of the system. They also talked about the six Monitoring and Video Surveillance Sector Centres.

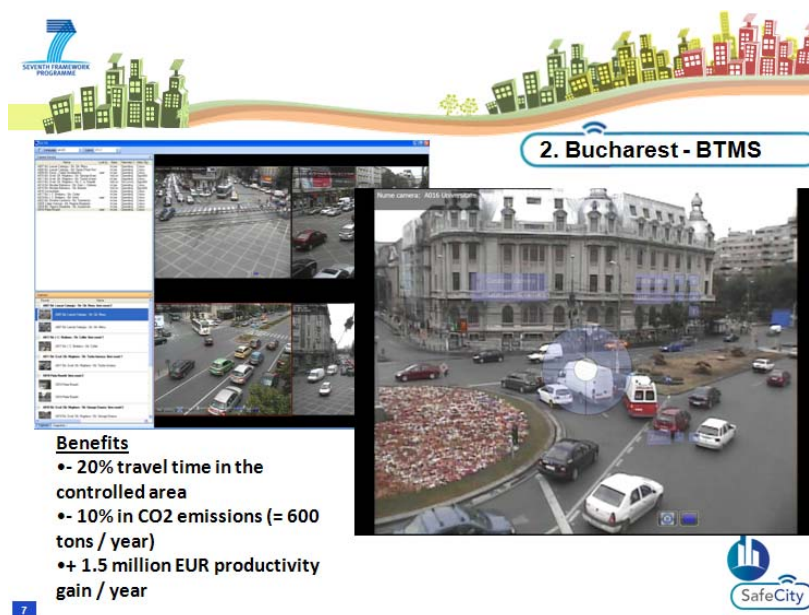


Figure 5 Bucharest BTMS system - WS

- Athens (Greece). Presented by Georgios Eftychidis, Centre for Security Studies, Kemea. He showed a high level description of Athens, then he listed the current infrastructure (Athens mass transit system, traffic monitoring CCTV network, the security CCTV network), he remarked the restrictions arose because of Personal Data Protection.

He also talked about the National Public Administration Network (SYZEFXIS) and the different operational centres.

Finally, he showed the Athens scenario they had proposed, explaining needs and requirements they had extracted of it.

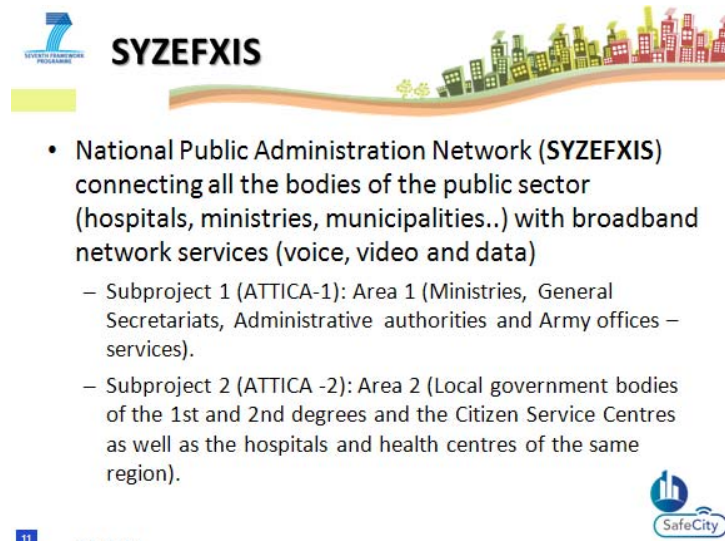


Figure 6 Athens SYZEFXIS - WS

- Stockholm (Sweden). Presented by Anders Hansson and Helena Grandlund, FOI. They showed a general overview of the city focusing on the Public Safety Agencies, Command and Control Centres and technical infrastructures, communication or surveillance systems. Current capabilities regarding situational awareness, mobile solutions and alerting technologies available in Stockholm were presented. They also pointed out the restriction due to the Swedish laws and regulations with respect to surveillance and gathering of personal data.

Finally, they showed the scenario they had proposed for Stockholm.

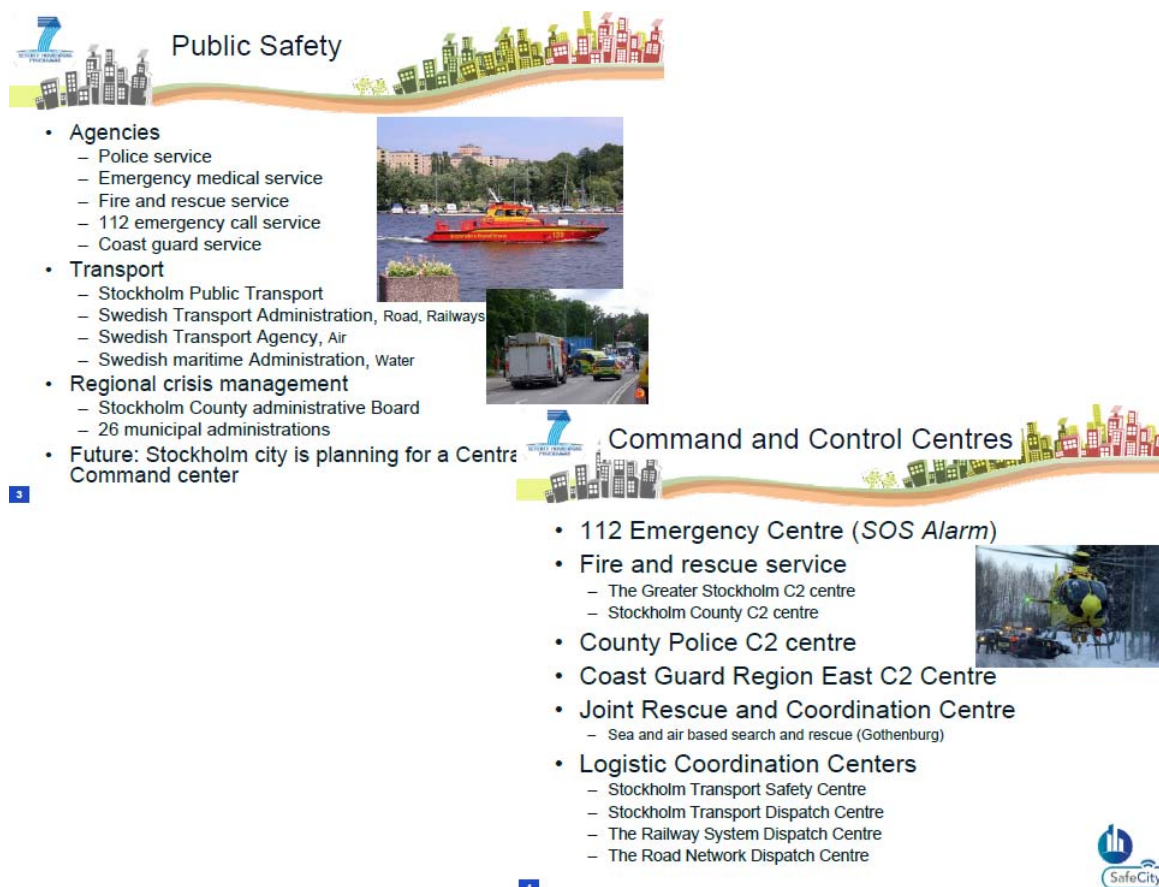


Figure 7 Stockholm Public Safety and C2 - WS

- Helsinki (Finland). Presented by Jussi Koivisto and Anssi Lehtinen. They showed a general overview of the city and its Police Department. They described their CCTV and traffic cameras system, remarking that Police was responsible authority of using, distributing, gathering and saving all the material.

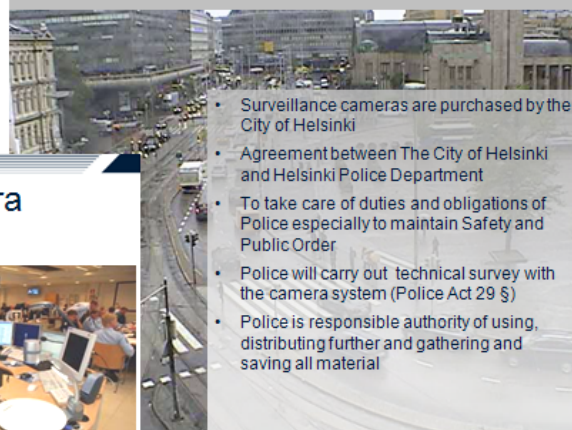
Helsinki Police Department

- State Police Department (not any Municipal Police Departments in Finland)
- founded 1826
- biggest Police Department in Finland
- staff about 1650, polices about 1300
- Police Commissioner is a Chief of Helsinki Police Department



Kaarti poli

CCTV - database in Helsinki



- Surveillance cameras are purchased by the City of Helsinki
- Agreement between The City of Helsinki and Helsinki Police Department
- To take care of duties and obligations of Police especially to maintain Safety and Public Order
- Police will carry out technical survey with the camera system (Police Act 29 §)
- Police is responsible authority of using, distributing further and gathering and saving all material

CCTV - and Traffic camera databases in Helsinki

CCTV Cameras:

- Main user is Helsinki Police / Operational Command Center
 - Possible future users: Customs, Border Guard, Rescue Department of Helsinki



Traffic cameras:

- User is Helsinki Region Traffic Management Centre (recording, controlling)
- 4 police officers working permanently
- 10 cameras available in HPD/OCC (tot. 40 cam.)



Figure 8 Helsinki Police and CCTV system - WS

- Obidus (Portugal). Presented by Pedro Antonio, Tekever. A general overview of Obidus was presented focusing on the actual public safety, he pointed out that they had no specific public safety applications so he remarked what the city expected from each SafeCity functionality area.

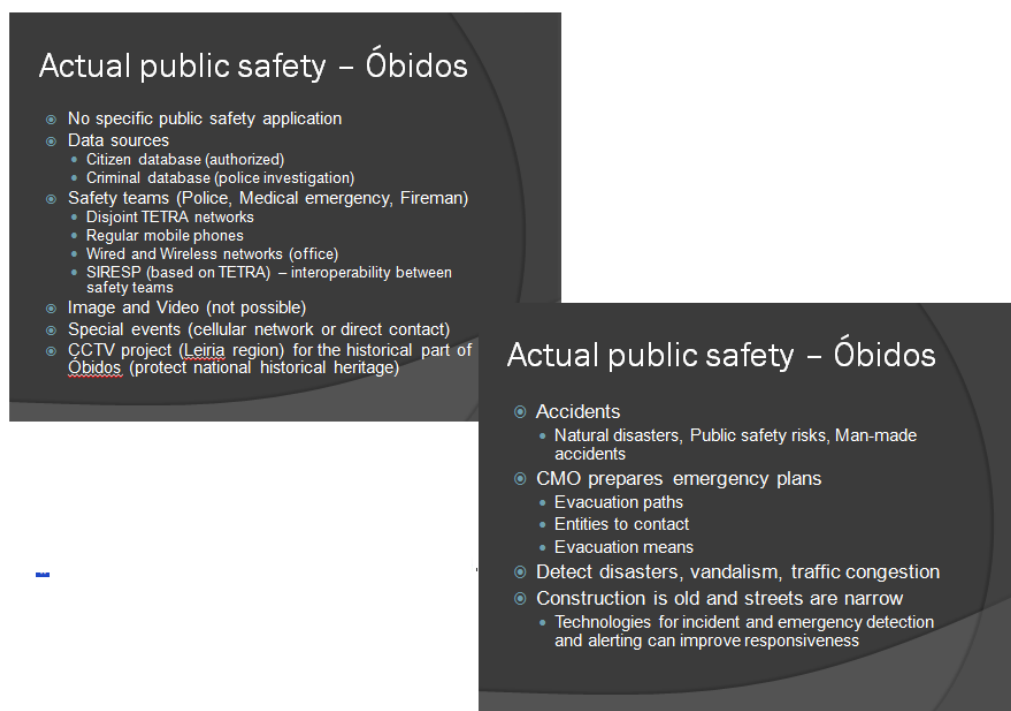


Figure 9 Obidus Actual Public Safety - WS

For each city, the end users feedback and comments were gathered.

The following slot was presented by Judith Pertejo, ISDEFE. She summarized the main outcomes arisen from previous steps to the WS via face-to-face meetings and questionnaires and listed the Public Safety and Security requirements collected in a structured and referenced way. These requirements were divided in four areas: situational awareness, command and control centre, alerting citizens and ad-hoc networks. Users' requirements have been gathered as workshop conclusion in section 3.4 of present document, as a consequence of including and modifying these requirements taking into account the WS feedback and discussions.

Finally, the SafeCity Applications were presented by Perez Gurel, Athena. It started with an overview of the high-level architecture that is being envisaged till the moment and practical vision and challenges regarding the future PoCs.

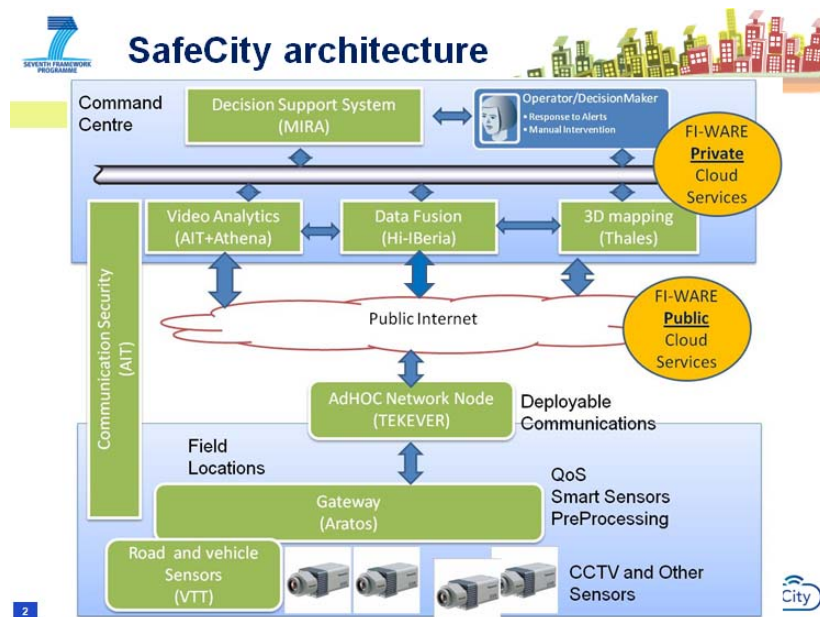


Figure 10 SafeCity architecture

A description of the 8 SafeCity applications was included, explaining in each case a general description of each one including the advantages the application provides.



Figure 11 SafeCity applications

For each case, the end users feedback and comments were gathered.

3.4 Workshop Conclusions

3.4.1 General overview

The scenarios Workshop was clearly fruitful and collaborative and held in a familiar and interactive atmosphere. Nearly ten different panelists from the Public Administrations and Public Safety Organizations from the 6 different cities and consultancies and technical experts from SafeCity Consortium provided the two points of view of current and future Public Safety systems in Europe.

Cities participation in the WS made clear the wide variety and strong similarities among the European cities, considering different necessities due to the inherent diversity of the cities under analysis: small (as Óbidos with several thousands of inhabitants), medium (between 100.000 and one million inhabitants as Athens, Helsinki or Stockholm) and large (more than 1 million, as Madrid or Bucharest). Larger cities count on widespread deployed infrastructure to support communication of different organizations. In general, all cities have invested resources to fight against their own critical problems. As example of key problems addressing in the cities it can be pointed out that northern EU cities are rather focused on enhancing traffic monitoring systems especially considering environmental issues. Southern EU cities use sensors and cameras also with other purposes than traffic monitoring, as Madrid, which head the list regarding video surveillance systems in public places. Small cities as Óbidus focuses its efforts on preservation of it heritage monuments and places.

Member States have different ethical regulations regarding handling Sensitive data. However, all of them are guided by European directives. In order to perform video surveillance in public places there are different authorization procedures in each State, some of them more complex or strict than others but in any case allowed for security purposes. Special mention should be pointed out regarding Greek's regulations, which currently forbid mentioned practices but actually there is a more permissive law under regulation.

The requirements summary showed a wide variety and structured list of necessities. A number of them are expected to be solved with certain Internet-based applications and technological computing capabilities that the project envisages in the following steps. Certain requirements proposed by the users cannot be achieved just with powerful networking capabilities but imply further investment on infrastructure and devices.

Maintenance and costs of the technological solutions can be concluded as being part of the main worries of the users, and therefore, it is highly required to be considered in the project.

Public Safety organizations presented clear interest regarding the 8 applications that SafeCity envisages to develop.

3.4.2 End-Users Requirements

As a result of the questionnaire [

Annex 2 – End user Questionnaire Template] analysis, the information gathered from personal interviews with end-users and the inputs generated during the workshop a set of users' requirements has been collected. In **Table 1** Public Safety and Security entities involved in User Requirements collection can be identified all the end-users.

Questionnaires filled by end-users can be found as annexes of the different cities deliverables [D2.1-6], depending on which city the end-users come from.

The questionnaire was designed according to the four areas as they have been used as a baseline for the requirements study:

- Situational awareness
- Command center Area
- Alerting citizens
- Ad-hoc networks

3.4.2.1 *Situational Awareness*

The content of the questionnaire addressed this area has been split in the following sub-areas:

- Intelligence Surveillance
 - Security
 - Citizen abnormal behaviour detection
 - Suspicious Objects detection
 - Safety
 - Environmental surveillance
 - Traffic surveillance
- QoS for surveillance systems
- Connectivity and integration for surveillance systems
- Sensitive data constrains

3.4.2.1.1 Intelligence surveillance

In the following table the end users requirements regarding intelligence surveillance are showed:

| Topic | Ref | Requirements | Details |
|------------------------------|-------|---|--|
| Media analysis | Ref 5 | Enable multi-modal input data | Ability to accept data from different sources (images, audio, video signal, sensor data). |
| Profiles definition | Ref 5 | Definition of knowledge databases | Definition of event profiles, modeling of suspicious targets to be detected. |
| Intelligence in Surveillance | Ref 1 | Alert rise software on the basis of images/video/data reading and knowledge databases | Ability to obtain meaningful semantic information from extracted data. Ability to identify an alerting event. |
| | Ref 1 | Active learning while detecting | Getting relevant insights from incoming data allowing continuous estimations and predictions. |
| | Ref 3 | Detection of malfunction of other equipment | Automatic repositioning of the video cameras in case of malfunctions detected to other equipment |
| | Ref 3 | Automatic repositioning of the cameras | Automatic repositioning of the video cameras if necessary. Eg the traffic values have been exceeded |

Table 2 Intelligence surveillance - Users Requirements

| Topic | Ref | Requirements | Details | |
|---------------------------------------|-------|---------------------------------------|--|--|
| Citizens abnormal behaviour profiling | Ref 1 | Identification of abnormal behaviours | Detection Targets | Potential Technologies |
| | | | 1. Disturbing concentrations , riots, demonstrations | <ul style="list-style-type: none">counting of peoplehuman avalanche’s detectionaudio detection |
| | | | 2. Criminal Activity, aggressive behavior, vandalism, robbery | <ul style="list-style-type: none">motions detectionreal time trackingbody gestures detectionhuman facial expressions detectionface recognition |
| | | | 3. Violation of restricted zones | <ul style="list-style-type: none">presence detectionbiometric identification |
| | Ref 1 | Guidelines for behaviour profiling | 1. Behaviour: <ul style="list-style-type: none">definition of “normal” activity deviation percentagelikelihood of next in sequence activities 2. Location: likelihood of events in different places3. Time: <ul style="list-style-type: none">likelihood of events depends on the time of the daydeviation in behaviour characterized in terms of time ranges. | |
| | Ref1 | Surveillance data type | <ul style="list-style-type: none">Video signalMetadata: Fixed camera location or camera ID, Date, time | |

Table 3 Citizens abnormal behavior detection - Users Requirements

| Topic | Ref | Requirements | Details | |
|-----------------------------|-------------|---|---|--|
| Objects detection profiling | Ref 1, 3, 5 | Identification of suspected objects | Detection Targets | Potential Technologies |
| | | | 1. Unattended objects <ul style="list-style-type: none">Bagslong time stationary vehicles (vans, delivery vehicles) in crowded areas or close to public institutions | <ul style="list-style-type: none">Object size detectionObject shapeCars features detection |
| | | | 2. Stolen cars | <ul style="list-style-type: none">Cars features detection (Licence plates, model, colour, etc.) |
| | Ref1 | Guidelines for suspect objects definition | 1. Location: intense surveillance in high risk areas (public places as airports) 2. Time: likelihood of suspected object depends on the time of the day and time being unattended. | |
| | Ref 1 | Surveillance data type | <ul style="list-style-type: none">Video surveillanceFixed camera location or camera IDDate, time | |

Table 4 Security – Objects detection - Users Requirements

| Topic | Ref | Requirements | Details | |
|--|-----------|--------------------------------|--|---|
| Environmental surveillance event profiling | Ref 6,7,8 | Targets | Detection Targets Potential Technologies | |
| | | | 1. Fires, smokes or health risks in public areas (critical infrastructures, parks, traffic tunnels, etc.) | <ul style="list-style-type: none">• Low-consuming fire detectors• Smoke detectors• Infrared cameras |
| | | | 2. Gas leaks, high contamination levels in public areas | <ul style="list-style-type: none">• Gas detectors• CO, NO and opacity sensors |
| | | | 3. Environmental impairments in traffic roads | <ul style="list-style-type: none">• Snow and ice detectors• Floods detectors |
| | | Guidelines for event detection | 1. Location: and Time 2. Usage of fire forecast algorithms 3. Integration with meteorological warnings | |
| | Ref 6,7 | Surveillance data type | <ul style="list-style-type: none">• Sensor data• Video images, EO Images• Geographic location,• Time, date. | |

Table 5 Safety – Environmental Surveillance - Users Requirements

| Topic | Ref | Requirements | Details | |
|--|-----------|--------------|---|--|
| Traffic Surveillance event profiling | Ref 2,3,4 | Targets | Detection Targets | Potential Technologies |
| | | | 1. Traffic congestion, congestion loads | <ul style="list-style-type: none"> Distinction of levels of traffic flow based on speed of the flow, flow variation and zone occupation Keep record of peak travel times and problematic locations (intersections) |
| | | | 2. Traffic incidents | <ul style="list-style-type: none"> Abnormal traffic flow detection |
| | | | 3. Restricted vehicle behaviour: <ul style="list-style-type: none"> vehicle going in opposite direction car stopped in forbidden area Irregular parking Slow moving car | <ul style="list-style-type: none"> motion detection and tracking presence detection |
| | | | 4. License plate recognition | <ul style="list-style-type: none"> Identification of suspect license Send an alarm in case of license in black list |
| | | | 5. Road condition detection <ul style="list-style-type: none"> disturbing objects in the road environmental disturbances pedestrians/cycles in the road or forbidden side-walks (e.g. inside a tunnel) | <ul style="list-style-type: none"> pot hole in the road surface recognition weather extreme conditions detection presence detection |
| | | | 6. Position of Police mobile resources on a map <ul style="list-style-type: none"> Vehicles Patrols | <ul style="list-style-type: none"> GPS tracking GIS applications |

| | | | |
|--|-------|------------------------|---|
| | | | <ul style="list-style-type: none"> • Policemen in service |
| | Ref 2 | | 7. Find the details of the certain vehicles (type, brand, plate numbers) |
| | Ref 2 | Surveillance data type | <ul style="list-style-type: none"> • Video images • Camera location (GPS coordinates) • Road identification: type of road, sector. |

Table 6 Safety – Traffic surveillance - Users Requirements

3.4.2.1.2 QoS for surveillance systems

| Topic | Ref | Requirements | Details |
|-------|------------|---|---|
| QoS | Ref 3, 5 | Bandwidth at least enough to cope with existing necessities | <ul style="list-style-type: none"> - Video Surveillance <ul style="list-style-type: none"> ▪ 8Mbps per stream for fixed cameras. ▪ 512 kbps per stream for mobile cameras. - Optical Character Recognition (OCR) data (license plates, GPS coordinates): 100kbps - Signaling : 25Kbps |
| | Ref 3,4, 5 | Strictest storage requirements | <ul style="list-style-type: none"> - Continuous 8Mbps video stream without compression for 7 days storage → 670GB per camera stream |
| | Ref 4 | Frame rate for video images reading tools | <ul style="list-style-type: none"> - 8-25 frames per second |
| | Ref 5 | Optimizing video storage | <ul style="list-style-type: none"> - Encoding video. - Video compression algorithms (MJPEG,MPEG-2,MPEG-4, H.264) |

Table 7 QoS for surveillance systems - Users Requirements

3.4.2.1.3 Connectivity and integration in Surveillance Systems

| Topic | Ref | Requirements | Details |
|---------------------|-------|--|---|
| Connectivity | Ref 5 | Network transmission cope with real-time services | Minimum latency of Video images display |
| Connectivity | Ref 5 | Connectivity with fixed and mobile devices. | City wide connection with fixed devices (cameras, sensors) and mobile devices (as smart phones, in-vehicle computers)* |
| Availability | Ref 5 | High network availability even for mobile devices | Currently, video signal from mobile devices to the C2 centres suffer from poor availability of public networks |
| Scalability | Ref 5 | Open and flexible solutions enabling scalability of surveillance systems | Handling thousands of cameras, environmental low-consuming sensors, other sensors |
| Devices integration | Ref 5 | Proper integration of video signal from fixed and mobile cameras. | Integration of different output formats depending on the <ul style="list-style-type: none"> Type of camera: optical, infrared. Camera brand (Sony, Panasonic, Axis, etc.) |
| | Ref 1 | Integration of heterogeneous sensor devices. | |
| | Ref 3 | Include processing capabilities at the sensor side. | |
| Integration | Ref2 | Integrate Traffic management with Traffic lights management | |

Table 8 Connectivity and integration in Surveillance Systems - Users Requirements

3.4.2.1.4 Sensitive data constrains

| Topic | Ref | Requirements | Details |
|----------------------------|------------------|--|---|
| Sensitive data constraints | Ref 2,5 | Sensitive data handling should cope with Ethical constraints | Personal data: criminal records, license plates, recorded images. |
| | Ref E3 | Physical system protection of sensitive data | Location limited to secure places (as police centers) |
| | Ref E3 | Visualization of public places recordings only allowed by selected authorities | Visualization restricted to authorities (generally, police officers)(*) |
| | Ref 5 | Sensitive databases cannot be directly connected to public network | Accessible by internal and secure requests. |
| | Ref E2 Ref E5 | Sensitive data should be securely encrypted for transmission over public network | E.g. License Plate Recognition (LPR) system of Madrid City Police: LPs are sent from vehicle cameras through public networks to control centers where identification of suspected LPs is performed checking internal databases. |

Table 9 Sensitive data constrains - Users Requirements

3.4.2.2 Command and Control Center Area

| Topic | Ref | Requirements | Details |
|-----------|-------|------------------------------------|---|
| Mobile CC | Ref 2 | Mobile Command and Control Centres | Mobile Command and Control Vehicles equipped with communication, imaging and computational facilities |

Table 10 Command and Control Centre - Users Requirements

3.4.2.2.1 Alarms management

| Topic | Ref | Requirements | Details |
|-------------------|-------------|---|--|
| Alarms filtering | Ref 4, 5 | High degree of reliability in “intelligent” detection | False alarms may cause the unnecessary costs and work. Guidance : less than 20% false alarms in traffic incident detection tools are accepted (Ref 4)(*) |
| Alarm correlation | Ref 4, 5 | Automated cross-references before alarm triggering | Historical data or 3rd party data sources |
| Alarms handling | Ref 3, 4, 5 | Provide full flexibility to model events to be alerted of | Proper user interfaces to re-defined alarms. Especially important when frequent malfunctioning detected |
| | Ref 4, 5 | Full flexibility for alarm triggering configuration . Enable a wide range of different procedures: from automatic functionalities to human intervention. | E.g. minimum human intervention for incidents detection E.g. human visualization for verification of abnormal behaviour in citizens/objects/traffic surveillance |
| | | Flexibility for configuration of visual /audio notifications | E.g. In M30 surveillance system <ul style="list-style-type: none"> • 960 cameras monitored by 4 operators • small squares for each camera • border in red colour when positive detection . Operator enlarges the image by clicking on it. |
| | Ref 4, 5 | Enable awareness of Software/hardware failure | Anomalous functionality of algorithms Anomalous functionality of equipment |

Table 11 Alarms management - Users Requirements

3.4.2.2.2 Surveillance Equipment management

| Topic | Ref | Requirements | Details |
|----------------------|-------|---|--|
| Equipment management | Ref 5 | Enable remote configuration of sensor devices. | Remote management of high resolution IP cameras of any vendor and model: <ul style="list-style-type: none"> • Optical Cameras: Pan Tilt Zoom (PTZ) , domo, 360º view of sight • Infrared cameras. • Wireless cameras, fixed |
| | Ref 4 | Flexible control of devices: centralized or distributed as required by the user. E.g. Pyramidal structure of M30 management architecture where Command Centre is at the top. Allow local logic at each control level. | |
| | Ref 4 | Necessity of service discovery mechanisms for initial set ups of deployed devices | |

Table 12 Surveillance Equipment management - Users Requirements

3.4.2.2.3 Visualization Requirements

| Topic | Ref | Requirements | Details |
|--------------------------|-------|--|---|
| Visualization Management | Ref 5 | Enable visualization of real time /recoded video. Simultaneous access from different operators. | |
| | | Multiple web-based consoles to configure and control video | |
| | | Enable scheduled and event-based video recording. “Record-now” feature while viewing live video | |
| | | Enable Video annotation capabilities. | |
| | Ref 3 | Enable operators to send data to other agencies | |
| Real time Tracking | Ref 5 | Real time tracking of suspicious target from one surveillance camera to another. | Triggered when positive suspicious detection. Stream synchronization mechanisms. required |
| | | Enable 3D visualization in the real time tracking of targets | Potential applications that ease the user development of 3D models of places with video surveillance cameras. |
| COP | Ref 6 | Common operational picture integrating multi-source data | Geo-spatial map of a city with various layers: street names, cameras locations, sensors locations, units deployed, etc. Enable zoom over any region of the map and watch live video displayed with a click on the camera |
| Maps integration | Ref 6 | Integration of input data with: <ul style="list-style-type: none"> • exiting GIS in C2 centres • commercial web services providing online and offline aerial, ortho image data as Google Earth & Google Maps | |

Table 13 Visualization - Users Requirements

3.4.2.2.4 Network Management

| Topic | Ref | Requirements | Details |
|-------------|-------|--|---|
| Reliability | Ref 4 | Full redundancy Command Centres structure | At all levels: storage devices, application servers, communication links, operators, etc. |
| Storage | Ref 4 | Efficient video storage | Optimization using dynamic file allocation. Flexible storage (different frame rates, durations, locations,) |
| | Ref 4 | Efficient data handling of large volumes of data | E.g. Data centre M30 C2 Centre employs Storage Area Network (SAN) solution for disk storage, a sharing storage philosophy that optimize the transmission of high volumes of data between servers and storage devices. |
| | Ref 4 | Simple storage administration | |
| | Ref 4 | Storage scalability | |
| Handling | Ref 4 | Full management of servers (application services, databases) and communication networks. | User management of network resources (BW, computing, storage) while using an application. |
| | Ref 4 | Dynamic configuration of different traffic flows | Virtual private communication links to separate traffic from different sub-systems or applications |
| | Ref 6 | Dynamic management of user groups accessing to web-based applications | Dynamic creation of private domains accessible through virtual private and secure connections by subscribed users |

Table 14 Networks management - Users Requirements

3.4.2.2.5 Share on-line services

Share online services with other Public Safety organizations; has been addressed in three different points:

- Surveillance systems integration
- Unified Emergency Response services
- On-line services for deployed units

Below, there is a picture which shows how the interaction among the different organizations would be:

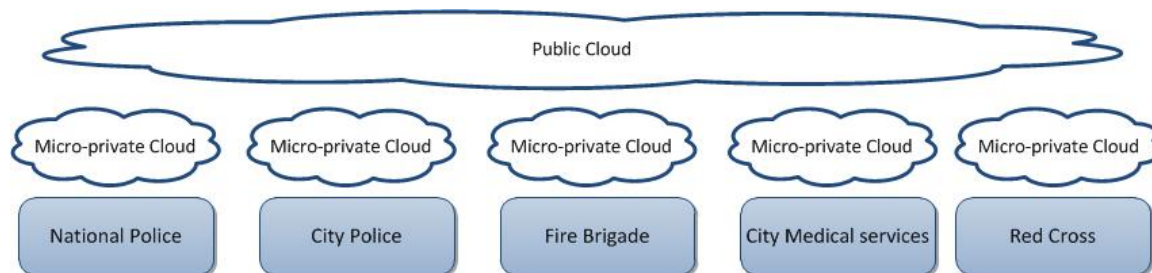


Figure 12 Share on-line services

| Topic | Ref | Requirements | Details |
|-------------------------------------|---------|--|---|
| Public/private cameras | Ref 7 | Integration of private CCTV systems for public safety and security purposes. | Video signal generated by Private operated cameras (private buildings, critical infrastructures, etc.) and police operated cameras of public spaces (streets, market squares) should be merged together to maximize surveillance capacities. |
| Citizen input | Ref 3 | Enable automated trustworthy surveillance information from citizens (fixed and mobile) | E.g. Video streams from incident place sent directly to systems operated by authorities over mobile networks and public Internet. E.g. Image of disturbing objects in a road. |
| Other PS organization inputs | Ref 4,5 | Integration of other CCTV systems handling by other PS organisms | E.g. In Madrid, CISEM receives M30 tunnel video signals |
| | Ref 4,5 | Share automated detections of larger incidents | Generally, not currently available. |

Table 15 Shared on line services- Surveillance integration - Users Requirements

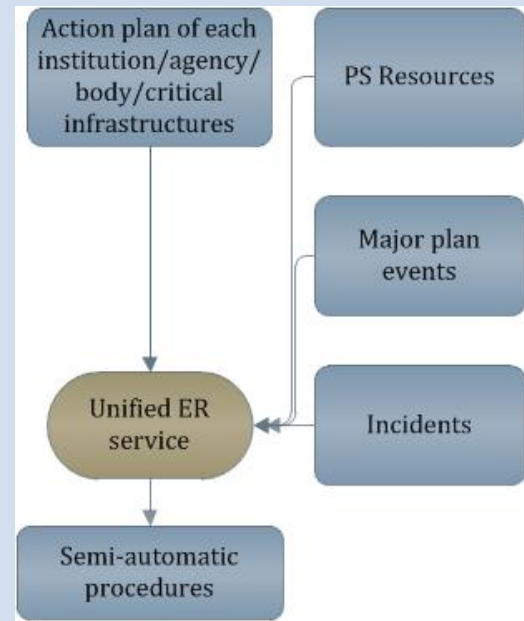
| Topic | Ref | Requirements | Details |
|-------------------------------------|------------|--|---|
| Unified Emergency response services | Ref 2, 4,6 | <p>Unified Incident Emergency Response.</p> <ul style="list-style-type: none"> • Enable coordination of emergency assets, e.g. at regional level • On-line secure access to the user application • Real time input: <ul style="list-style-type: none"> ○ PS resources, real-time location ○ PS regular actuation procedures ○ Ad-hoc security procedures of critical infrastructures ○ Incidents information ○ Major plan events • Semi-automated plan as output: <ul style="list-style-type: none"> ○ Assignment of right resources that should attend a detected incident (Madrid SITE*) ○ Indication of ad-hoc optimal procedures for each responder <ul style="list-style-type: none"> ✓ route calculation system ✓ Nearest access points/emergency exits ✓ Crucial nearby places (hospitals) | <p>Benefits pursued:</p> <ul style="list-style-type: none"> • reduce ER time • standardize procedures and protocols • seamless coordination • enable shared use of resources  <pre> graph TD A["Action plan of each institution/agency/body/critical infrastructures"] --> UER["Unified ER service"] B["PS Resources"] --> UER C["Major plan events"] --> UER D["Incidents"] --> UER UER --> E["Semi-automatic procedures"] </pre> |

Table 16 Shared on-line services- Unified Emergency response activities - Users Requirements

| Topic | Ref | Requirements | Details |
|-----------------------|---------|---|--|
| Over private networks | Ref 2 | Require interoperability with private networks (PMR, TETRA and TETRAPOL) offering mobile connectivity to PS members in the field | Enable sending low data rate messages (voice commands and short instantaneous messages) from C2 centres to targeted PS members in the field (FRs attending an incident, surveillance agents, patrol units) |
| Over public networks | Ref 6 | Require interoperability with public networks (wireless hotspots networks, GSM/GPRS/UMTS/4G) offering mobile connectivity to PS members in the field. | Enable remote access to surveillance video through internet browser (password protected). E.g. Swedish fire-brigades access video surveillance data of the incident area through mobile devices. |
| | Ref 5 | | Enable remote access to surveillance video through internet browser (password protected). E.g. Swedish fire-brigades access video surveillance data of the incident area through mobile devices. |
| | Ref 6,8 | | Enable transmission of video images from mobile devices of FRs or patrol units |
| | Ref 3,8 | | Remote access to Common Operational Pictures in mobile terminals of first responders in an emergency |

Table 17 On-line services for deployed units - Users Requirements

3.4.2.2.6 Security Management

| Topic | Ref | Requirements | Details |
|---------------------|-------|--|--|
| Security management | Ref 5 | Enable different security levels for database access and storage | Sensitive data requires the highest security level (password-protection and other mechanisms that guarantee the security requirements) |
| | Ref 5 | Flexible set up of security level | |
| | Ref 5 | Monitoring of sensitive data entries . Keep access records. | Allow checking identification of entries, access statistics. |
| | Ref 5 | Full security management of sensitive & non-sensitive databases | Full management queries, storage, and transmission of sensitive information.(*) |

Table 18 Security management - Users Requirements

3.4.2.3 *Alerting citizens*

| Topic | Ref | Requirements | Details |
|-----------------------|---------------|--|--|
| Ethical exigency | Ref E1 | Guarantee that citizens are aware of entering in surveillance place | E.g.: cameras with laser illuminators associated to cameras in order to advise people involve in incidents E.g.: Internet-based access to surveillance images (enable previous automated blurring of other citizens' faces) |
| Public address system | Ref 3 | Automated advertising through traffic electronic panels (human supervision) | Informing of traffic restrictions, alternative routes, estimated period of unavailability. |
| | Ref 2 | Integration with megaphone systems | E.g. in tunnels, critical infrastructures |
| Public networks | Ref 5 | Enable automated identification of fixed and mobile terminals' location | Allow targeting alerts to citizens located in affected area |
| | Ref 5 | Send automatically generated instantaneous messages (SMS alerting) to targeted citizens mobile phones | E.g. bomb attacks, fires, evacuations, adverse weather conditions, etc. are critical incidents where these tools is critical. |
| | Ref 5 | Enable automatically sending alerting voice messages to targeted fixed terminals | |
| Internet | Ref 5 | Enable Internet-based alerting through E-mail/social network | On-line message warnings for subscribed citizens |
| | Ref 5 | Ease the integration of alarm messages into relevant web sites (Governmental sites, big enterprises sites). | On-line message warnings for every user. |
| Media | Ref2 Ref 5 | Enable broadcast warnings on TV and radio | |

Table 19 Alerting citizens - Users Requirements

3.4.2.4 *Ad-hoc Network Area*

| Topic | Ref | Requirements | Details |
|-----------------------------|-------|---|--|
| PS comms. in the field | Ref 5 | Ensure low data rate FRs communications in the field (voice and localization). | IP-based ad-hoc networks should have proper interfaces with radio communication networks. Nodes should be easily deployed after fixed ICT infrastructure is destroyed or not working properly. |
| | Ref 2 | Enlarge coverage of private networks (PMR, TETRA) | - |
| | Ref 2 | Ensure interoperability with legacy terminals | Different FR would use their own terminal, ensure the communications among them. |
| | Ref 5 | Ensure high data rate communications (video stream and sensor data) between C2 centres and deployed units. | Wireless communication nodes (Wifi, Wimax protocols based) can likely provide broadband services in the field with integration with 4G /LTE public mobile networks or prioritized services over 3G networks. |
| Surveillance devices comms. | Ref 5 | Ensure high data rate communications between video cameras and processing centers | As high-resolution IP cameras may require additional communication infrastructure (wired or wireless). |
| | Ref 5 | Ensure connectivity of remote wireless sensors with processing centers. | Deployment of wireless nodes to enable internet access to devices with proper interfaces. |
| Robustness | Ref 2 | The network should not fall in case any node fails. | - |

Table 20 Ad-hoc Network - Users Requirements

4. Key conclusions of European Public Safety Systems

4.1 PS Characterization in EU cities

The six cities deliverables have been deeply analysed in order to have a clear and concise overview of what is the state of art of Public Safety systems in Europe.

Depending on each city, Public Safety agencies consider more important certain areas according to their specific context and exigencies and, therefore, those areas are more developed, taking into account laws and regulation, population, weather conditions, etc.

Madrid counts with a vast CCTV surveillance system managed by CISEVI (Integrated Video Signal Centre), integrating images of City Council facilities, traffic cameras and street surveillance. Beside, M30 tunnels have a great technological deployment including number plates tracking, calculation of access points in case of accident, environmental monitoring.

Bucharest holds BTMS which is a modern system used in the city for the management of road traffic. Bucharest city does not count with any system to control citizen behaviour.

Athens has many restrictions due to ethical constrains which produces strict law in terms of video surveillance, generally it is not allowed to have CCTV system for surveillance activities if people are recorded. In Athens due to the Olympics Games in 2004 many application were carried out to increased safety during those days but they are no longer in use: Security CCTV system or Intelligent Traffic System (Traficon), traffic surveillance is nowadays carried out by operators.

Stockholm owns cameras for surveillance in Public Transport, allowing to control if someone enters the track but also if there are people moving at the stations. Besides, there are also road weather stations.

Helsinki has CCTV cameras in the city managed by police for citizen surveillance. Unlike other cities, in Helsinki due to the frequent extreme weather conditions they have systems in order to control traffic and roads conditions.

Obidos is the smallest city that has been studied. The deployment of technology in the city is non-existing but is expected that all the historical area will be equipped with CCTV system.

4.1.1 Situational Awareness area

Most of the cities have applications or systems to improve the knowledge about what is happening in the city. The main objectives are:

- Citizen surveillance: historical and security buildings (Police, Public entities, etc.), commercial or touristic area, etc.
- Road track surveillance, for incidents and traffic management or road conditions due to weather.
- Environmental Monitoring

Sensors

Most of analysed cities have the infrastructure of CCTV systems. Typically IP and non-IP fixed cameras remotely controlled by the Police Command Centres. Stationary CCTV cameras scattered in the city are connected to the police command centre by a private data network usually comprised by broadband wired connections based on fiber optic solutions¹. Depending on the city the CCTV system is used for citizen surveillance, road track surveillance or both, constraints due to ethical aspects come up.

Apart from the cameras for Road track surveillance there are sensors deployed around the different cities to control the conditions of the road as asphalt buried sensors counting traffic values, temperature, wing speed or humidity.

In terms of environmental monitoring there are also different kinds of sensors which mainly are in charge of determining the quality of air: temperature sensor, smoke sensors, CO, CO2, SO2, O3, etc.

Detections

In video surveillance systems there are no automatic capabilities for citizen surveillance. Usually the way the information is processed is through police officers who are observing the images in real time, overwhelming the operators. However, some features help the operators to control and visualize the images as publishing selected images on a video wall, viewing images on the operator's screen, automatic recording, etc. the availability of some or all these features depends on the city.

Regarding Road track surveillance the applications seems to be more developed as some cities counts with systems for best manage the traffic (BTMS, Bucharest); System to detect automatically where are traffic conditions (not in used nowadays) (Athens); automatic plate recognition which enables to identify stolen cars and M30 road incident management which automatically detects accidents within the tunnel(Madrid); automatic speed surveillance cameras or illegal use of bus lane (Helsinki) or identification of someone entering the track and people moving in stations at night (Stockholm).

In terms of environmental monitoring the cities have automatic equipment which measure and provide continuous information about the quality of the air, through different stations scattered around the city in order to provide human health protection.

Infrastructure

All the cities have dedicated networks to transmit the information from the devices deployed in the city to the Command Centres; depending on the city, the networks belong and are managed by different authorities. The technology that mainly predominates is Optical Fibre as the case of Athens, Madrid and Bucharest which manage its own private optical fibre rings.

In some cities, there have been difficulties to gather further information for private ICT network as is this type of information is restricted to only authorized persons, not having been able to get more details.

¹ In the Madrid case, new wireless 360° HD stationary cameras are starting to be deployed in certain areas of the city.

Flow of information

Once the information is captured through the different sensors distributed around the cities, each public safety body in charge of these sensors is responsible of managing the information coming from them and provides it to the rest of agencies upon request. Nowadays there is not a mechanism that allows a distributed flow of information. However, Stockholm promotes an online application to enhance situational awareness, this way the information is shared among different public safety agencies without need of request to other agency, making the flow of information more dynamic and flexibility reachable.

To finish, just point out the connection between descent of criminality and technology. This fact can be clearly observed in Madrid case [Ref D2.1] where the criminality rate dramatically decreased since the establishment of the Strategic Plan *Madrid Seguro*, started after the Madrid bombings terrorist attack in 2004. *Madrid Seguro* program included technological achievements related to public safety that contributed actively to make Madrid safer. Several facts confirm that tendency. On one side citizens ensure the currently feel safer in Madrid as stated by the Spanish Security Observatory organization. Secondly, the reinforced video surveillance system in certain troubled areas of Madrid highly decreased the demand of police intervention.

4.1.2 Command Centre Area

First of all, one main characteristic it should be highlighted is the presence of regional and national organisms dealing with similar Public Safety and Security issues in each European city. PS organizations attending an specific city could be City/Municipal Police, National police attending the corresponding region, different Fire Brigades, Rescue agencies, Medical services managed by public authorities, other medical services as Red Cross, etc.). Each entity has its own Command Centre or headquarters, connected to the Emergency Command Centre of the city.

In some cities authorities are trying to centralize all the information into one Centre in order to get more organized response to critical situations. Some examples are described following:

- CISEM and CISEVI in Madrid. CISEM integrates information, systems and people allowing seamless coordination among emergency response teams, while also giving emergency managers the understanding and insight required to better assess needs, prioritize and coordinate actions, and proactively deploy assets to address, and potentially prevent, multiple, complex incidents. CISEVI, integrated with CISEM, and centralized video system receives video information
- Road Network Dispatch Centre in Stockholm which manages information from Public transport system and road network system allowing forward video stream from their cameras to other command and control centres.
- There are also new initiatives as ESMSBM in Bucharest which aims at developing an integrated and unitary system for the management of emergency situations.

4.1.3 Alerting Citizens area

Alerting citizen is mainly carried out using TV, radio or mass media channels or through acoustic and in some case optical signals. In general, automatic alerting systems are not used by any city; the actuation

procedure is declaring the emergency and activating the emergency system by the agency in charge which vary depending on each city, although, in general are local authorities' Emergency center.

The importance of Internet within this area is persistently increasing. Several public agencies used web applications, as their own web site or even social applications, in order to transmit emergency situations to the citizens. Hellenic Police web site is used for non-urgent cases, Helsinki Turva fi Portal which helps to enhance the information of incident and reduces the amount of non-critical calls to 112 emergency numbers.

4.1.4 Ad-hoc Networks area

Ad-hoc networks is not a very developed area in the current time by the studied cities.

Some cities own Mobile Command Control Centre to be deployed in case of emergency situations which objective is to ensure communications in emergency situations with different interfaces as Mobile phone interfaces: GSM, UMTS and CDMA, analogical radio UHF/VHF, TETRA communications, VSAT satellite, Broad Band Wireless, etc. The deployment of this kind of "nodes" helps to increase the perception of safety among the citizens.

On the other hand, thanks to the availability of multiple cellular networks, private networks as TETRA or WI-Fi spots communications setups can be establish in different areas.

4.2 Social, ethical and legal considerations

As result of interviews, questionnaires, workshop and the analysis of the cities deliverables social, ethical and legal considerations have arisen, depending on each one the rules and therefore the requirements coming from each are completely different.

While safety and security of all public places should be maintained, ethical implications arise in order to guarantee the privacy of citizens.

Member States regulations present different rules and conditions that legally restrict these video surveillance systems. Other legal instruments for monitoring video surveillance are Data Protection Authorities, jurisprudence, recommendation of European institutions and national institutions as Data Protection Authorities.

Below some regulations arise from the cities studies can be observed but the main research regarding social, ethical and legal consideration have been carried out within D7.7.

| Reference Number | Regulations or Directives |
|------------------|---|
| Ref E1 | European Directives <ul style="list-style-type: none"> • Directive EC 95/46, • Directive EC 2006/24, • Directive EC 2009/136. • European Union Agency for Fundamental Rights. |
| Ref E2 | Spanish regulations: <ul style="list-style-type: none"> • Personal information Protection Law 15/99 (regulates the use of video cameras); • Right to Honor Civil Protection, personal and |

| | |
|--------|---|
| | family privacy and image Law 1/1982 |
| Ref E3 | Greek regulations: <ul style="list-style-type: none"> • Law 2472/1997 • Law 3471/2006 |
| Ref E4 | Swedish regulations <ul style="list-style-type: none"> • Allmän kameraövervakning (1998:150) • <i>personuppgiftslagen</i> (1998:204) • <i>offentlighets- och sekretesslagen</i> (2009:400) • <i>Lag om säkerhet i vägtunnlar</i> (2006:418) |
| Ref 5 | Finnish regulations <ul style="list-style-type: none"> • Police Act (493/1995) <ul style="list-style-type: none"> ○ Police Act section 29 ○ Act on the Processing of Personal Data by the Police (761/2003) • Personal Data Act (523/1999) |
| | Romanian regulations <ul style="list-style-type: none"> • <i>Law 102/2005</i> • <i>Law 102/2005</i> • <i>Law 677/2001</i> |

Table 21 Regulations and Laws

As result of all the work carried out during Task 2.1: interviews, questionnaires, Workshop and deliverables analysis some requirements have arisen considering Social, ethical and legal considerations:

| Reference Number | Regulations or Directives | Details |
|------------------|--|---|
| Ref 2, 4, 5 | Sensitive data handling should cope with Ethical constraints | Personal data: criminal records, licence plates, recorded images |
| Ref E3 | Physical system protection of sensitive data | Location limited to secure places (as police centers) |
| Ref E3, 5 | Visualization of public places recordings only allowed by selected authorities | Visualization restricted to authorities (generally, police officers)(*) |
| Ref 5 | Sensitive databases cannot be directly connected to public network | Accessible by internal and secure requests. |
| Ref 5 | Sensitive data should be securely encrypted for transmission over public networks | E.g. License Plate Recognition (LPR) system of Madrid City Police: LPs are sent from vehicle cameras through public networks to control centers where identification of suspected LPs is performed checking internal databases. |
| Ref E3, Ref E4 | Installation of surveillance cameras should comply with | Use of cameras should always be an alternative, when no less intrusive way is |

| | | |
|------------------|--|---|
| | regulation procedures | feasible to achieve the final aim. Analysis of following criteria: <ul style="list-style-type: none"> •Application (is it possible to achieve the objective through the use of video cameras?), •Need (is it the only feasible way?), •Test of proportionality (does it cause more harm than good to the citizens concerned?). |
| Ref E2 Ref E3 | Type of surveillance targets allowed with CCTV systems | Traffic monitoring and criminal prevention. NOTE: Greek law only allows traffic monitoring (new more permissive law under development)(*) |
| Ref E1 Ref E2 | Dynamic masking technology in CCTV cameras | A public space surveillance system cannot have as a “side effect” the surveillance of private spaces. |
| Ref E2 Ref E3 | 7 days is the maximum storage time | Could be exceptionally enlarged under jurisprudence request. NOTE: Greek law also regulates expiration time of private sector(**) |
| Ref 3 | Consider potential risks of misuses of the system | The major risk for the use of this system is the risk to be used in other purposes than the legal ones and the ones for which it was designed. In this respect, there have to be issued criteria to identify the intrusions or the use in other purposes. |

Table 22 Requirements from Social, ethical and legal considerations

Video surveillance system might be the area that major ethical constraints arise when it used as citizen surveillance system in public places

These video-surveillance systems are used primarily for traffic monitoring purposes. However, few European cities of the 6 analyzed have citizen video-surveillance systems in public places due to strict constraints of their National regulations regarding Personal Data Protection.

- Madrid: there are specific procedures that regulate the installation and use of the video surveillance systems in public places. The installation shall be authorized by the Madrid Commission of Surveillance Guarantee and each of them should pass the test of proportionality which is essential to determine the legality of any restriction on fundamental rights. Approval of Security Area of Madrid City Council is also required.
- Bucharest: the CCTV network is installed just for traffic purposes.
- Athens: this case is one of the more restrictive as CCTV network installed in Athens are just allowed for traffic law enforcement as it is not allow to use the images for other purpose although , in any special case the information coming from CCTV system might be used for security tasks.

- Stockholm: the main objective of the CCTV system install along the city is traffic surveillance although there are few applications regarding citizen presence. For camera installation and surveillance of cameras directed at public places the Public camera surveillance act is the most important regulator and the Stockholm County administrative board grants the permissions and supervises the use of the cameras.
- Helsinki: the main issue is the different between public and private area, distinguishing the domestic areas in order to avoid intrusion, it is not possible to monitor domestic areas without special conditions and permits. In case of installing cameras in public areas, Police need to notify the existence of this system.
- Obidos: no main ethical constrains although nowadays there is no CCTV system install for any purpose.

4.3 Challenges arisen from User Requirements

This section synthetizes the main issues originated from cities analysis and user requirements that potentially drive the following steps to be taken in the project.

Limitations of CCTV Systems:

CCTV systems present certain inefficiencies nowadays. There are hundreds of cameras in medium cities such as Bucharest, Athens, Stockholm or Helsinki and thousands in larger cities as Madrid. With the increasing number of surveillance cameras, there is not enough operators (usually, police officers) to visualize all real time video images.

Intelligence surveillance systems are required to solve this situation and automatize the process efficiently. Certain video analytics algorithms are fruitfully installed for traffic surveillance purposes. For instance, Madrid M30 system (deployed in a tunnel of 4km with 960 video cameras) automatically detect vehicles which are stopped or going in the opposite direction, or citizens/cycles going through the road track or road side (even though the false alarm ratio is high reaching 20%). However, crime fighting cameras dedicated for Public Places monitoring (citizens, objects, etc) do not have any capabilities related. A new generation of analytic is needed, with more capabilities. *Automated video data analysis tool* envisaged by SafeCity aims at triggering human action when potential suspicious happenings. It aims at analyzing video inputs in near-real time looking for suspicious objects with orphan object detection, suspicious entries with intrusion detection, suspicious people based on anomalous pattern detection and face recognition for wanted objectives, etc. **For this purpose the user requirements collected within situational awareness area are of the utmost importance.** Reaction is much more timely and efficient. This application even limits progression of potential dangerous situations. There are a number of technical issues to be solved. Information extraction from video images should be enabled by multimedia analysis tools. Also the definition of knowledge databases or reasoning rules that help deciding a critical situation is happening and real-time processing are other main technical issues to be tackled.

Another limitation crucial for this type of systems is that the operators must manually change the camera to keep the moving target in the monitor which is highly inefficient and sometimes leads to miss the target. SafeCity is working on a real-time tracking capability that aims at providing the operator proper visualization from the right cameras, even with 3D visualization. This may imply a global situation understanding where the operator can navigate and see tracks in an easy and automated way. Artificial intelligence capabilities are envisaged to anticipate the location of an object or a person when no real-

time video signal is received. Key challenges to be highlighted are the synchronization of different video signal inputs, integration of different CCTV systems (e.g. Metro cameras handled by a private entity – Police CCTV cameras in public places) or the realization of 3D models of surveillance areas.

Limitations regarding Security

Along this document Security problems have been arisen as consequence of Social, ethical and legal constrains. Public safety agencies have specific requirements regarding sensible data security. For instance, physical system protection of sensitive data is compulsory; sensitive DB cannot belong to the public cloud, it should be located in secure places; furthermore, sensitive DB or devices which generate sensitive information cannot be access through public network, they are only accessible by requests coming from internal private network.

Cloud services and capabilities could provide a lot of benefits to PS organization; Private cloud services might cover PS necessities. However, considering the above recommendations, certain restriction should be taken into consideration.

Servers that store sensitive databases should be located in a secure domain and database checking should be restricted to highly secure environment, internally. Private cloud services need to be set up separately for Public Safety organizations in a way that network resources (computing, storage) are desired not to be shared with other market-oriented services.

Access to sensitive data should be highly restricted to authorized users through password-protection and other mechanisms that guarantee the security requirements. Applications that require the sensitive databases requests should be subject to strictest security mechanisms. Other applications not handling non-sensitive databases may just require PS entities will be subscribed to Private Cloud services.

Additionally, dynamic set up of security level while database access, storage and transmission is required and also different encryption levels of storage information and of the transmitted information should be allowed.

Necessities regarding QoS of Communications

In some cases Public safety agencies have to rely on Public Mobile Networks to connect different sensors scattered around the city, as cameras installed in patrol vehicles in Madrid, or even to establish communication being communications vital part of FR's operations as it connects them among them or with the Command Centre all the time providing important information that is necessary for their own well-being and for the operation development. It seems essential to establish priority communication at least during crisis situation for Public Safety agencies so QoS is guaranteed.

On the other hand, Private data networks are massively used by Public Safety and Security organizations since they provide assured level of performance, many cities have dedicated networks which transmit the information from the devices scattered around the city to the different C2.

Integration

Several solutions might arise in order to comply with end-users requirements and necessities, and enhance Public safety. So another problem can come up as the new solution can be incompatible with the ones that are currently in used. All the system and solutions have to be easily integrated with the

actual ones as both would be coexisting. Moreover, integration among system handled by different agencies is also needed.

Considering end-user comments it can be noticed that the problems usually detected is connected to the large number of systems they use. Some end users have more than 20 passwords for systems they need to connect to in order to do their work. This is time consuming but feasible during ordinary work, but a severe hinder in emergency events, when time is scarce, the risk high and cognitive work is needed for the event itself.

Massive alerting systems

Citizen alerting is a means of mass alert notification that has the ability to find citizens anytime, anywhere, and on any device. These systems must have the ability to reach people and guarantee that citizens are aware of crisis situations.

Nowadays, the use of mobile and other electronic devices, as notebook or computers is highly increasing, making use of email, social network or other applications. Some solutions that might solve the problems could be:

- 1) Cell broadcast messaging, it would provide with SMS to multiple users in a specific area
- 2) On-line services for alerting citizens taking advantages especially of the use of social network and other website and applications.

It should not be forgotten the highly impact of mass media which offers broadcast to the public.

Interoperability

There is a tremendous lack of interoperability among different Public Safety organizations generated by the private closed solutions in used.

Cloud computing and storage services present clear advantages that could enhance the Public Safety and Security field capabilities. Cloud services have minimum costs since no need for initial investment in infrastructure is foreseen and because they present high flexibility. The adoption of cloud technologies internally within PS organizations may provide them a lot of benefits. What is more, cloud computing and storage services would potentially provide crucial benefits in this interoperability issue.

However, considering Private Data protection restrictions regarding handling sensitive data, private cloud services extremely secure are required to efficiently cover PS necessities. Some of these restrictions imply that servers that store sensitive databases must be physically located in a secure domain and database checking should be restricted to highly secure environment, internally. Private cloud services need to be set up separately for Public Safety organizations in a way that network resources (computing, storage) are desired not to be shared with other market-oriented services.

Several on-line applications of interest to the users are a

- Unified Surveillance System: possibility of creating a Common operation Picture of the situation of the city or an emergency, where surveillance devices of different Public Safety organizations merged into a unique storage being on-line accessible from fixed or mobile sites from PS members.

- Unified Emergency response system that enable the global coordination of emergency assets of a city or a region (see Unified Emergency response services of page 32)
- Enable data collection from third parties (even citizens' devices).

Surveillance Sensors

Most of current Public Safety applications are focused on responding phases of incidents/emergencies but there is an enormous lack of anticipation and prevention capabilities. Public Safety organizations envisage increasing the number of deployed fixed and mobile sensors which potentially increase the M2M communications within the networks.

Furthermore, future Public Safety capabilities can potentially take advantage of millions of sensors and actuators (including persons using their mobile phones to sense and interact with the environment), should be able to “listen” and “comprehend” what is happening all over the city to thus make better decisions and provide the right information and services to its inhabitants. “Ubiquitous Sensor Networks” (USN) is a relevant term which is used to describe a network of intelligent sensors that could be used to provide context-aware information and knowledge services to anyone at anywhere, and anytime, for anything. USNs would support decision makers in early detection of a possibly catastrophic event. USNs have the ability to control and monitor large physical environment, even in potential harmful places for humans. The use of sensor network information in Command & Control systems has two major advantages: it raises situational awareness of decision makers with the incident detection in real-time, and it reduces the response time between incident detection and proper assignment of first responder forces (e.g. ambulance, firefighters, police, etc.) to a critical situation.

However, the lack of USN integration into legacy systems is mainly due to technical (e.g. data routing, processing, heterogeneity) and security-related (information confidentiality, integrity) issues introduced by USNs. To enable the use of a common sensor and actuator information infrastructure across the city one must guarantee i) the secure and reliable access to sensor and actuator information services for multiple players and ii) the efficient sharing of information. The challenges to achieve this vision include the following.

- Technical challenges as vast amount of data, high degree of automation, real time control and unified access to data.
- Sensor information enablement, aggregation and collection of data directory services, data brokering and service composition, information federation, privacy and integrity protection.

Challenges arisen here are related also to gateway capabilities at the sensor side that aims at enhancing pre-processing capabilities and therefore, help reducing the amount of traffic through the network, and at enhancing flexibility of interfaces suitable to handle a wide set of heterogeneous devices. Flexible security mechanisms should be available considering the wireless nature of sensors and different privacy restrictions depending on the type of information.

SafeCity aims at helping to solve a number of these challenges within the project progress.

5. Annexes

5.1 Annex 1 – Public Safety Scenarios Template



SafeCity -
D2.x-[partner]-[city].

5.2 Annex 2 – End user Questionnaire Template



SafeCity_Questionnaire-v5.doc

5.3 Annex 3 – Workshop Agenda

| | | |
|-------------|--------------------------|--|
| 09:30-10:00 | Registration | |
| 10:00-10:05 | Welcome | Workshop Welcome Mr. Diego Giménez, SafeCity Project Coordinator, R&D Projects Manager at ISDEFE |
| 10:05-10:15 | Individual presentations | Individual presentation of each participant and the role which they play in the project Participants: SafeCity members and the whole audience |
| 10:15-10:30 | SafeCity overview | General overview of SafeCity project Mr. Diego Giménez, SafeCity Project Coordinator, R&D Project Manager at ISDEFE |
| 10:30-10:45 | Use Case Cities | Madrid, Spain Ms. Sara Gutierrez, Innovation Department of Madrid Police Department Security Services |
| 10:45-10:55 | | Feedback of the audience |
| 10:55-11:10 | | Bucharest, Romania Mr. Valentin Ifrim, Director of the IT and Equipment Administration Directorate within Bucharest Mayor Office Sector 2 |
| 11:10-11:20 | | Feedback of the audience |
| 11:20-11:50 | COFFEE | |
| 11:50-12:05 | Use Case Cities | Athens, Greece Mr. Georgios Eftychidis, Security applications expert at KEMEA |
| 12:05-12:15 | | Feedback of the audience |

| | | |
|--------------------|-------------------------------------|--|
| 12:15-12:30 | | Stockholm, Sweden Mr. Anders Hansson, Senior Scientist at FOI |
| 12:30-12:40 | | Feedback of the audience |
| 12:40-12:55 | | Helsinki, Finland Mr. Jussi Koivisto, Police Sergeant at Helsinki Police Department |
| 12:55-13:05 | | Feedback of the audience |
| 13:05-13:20 | | Obidos, Portugal Mr. Pedro Antonio, Senior Researcher at TEKEVER |
| 13:20-14:30 | LUNCH | |
| 14:30-15:30 | SafeCity work and invitees feedback | Questionnaires results Ms. Judith Pertejo, R&D Researcher at ISDEFE |
| 15:30-16:30 | | SafeCity applications and end-users feedback Mr. Perez Gurel, Business Development Manager at Athena GS3 Security implementations |
| 16:30-16:45 | Wrap-up and conclusions | Workshop main conclusions. Closure. Mr. Diego Giménez, SafeCity Project Coordinator, R&D Project Manager at ISDEFE |

5.4 Annex 4 – Attendees List

| | NAME | COMPANY | IDENTITY CARD | SIGNATURE |
|---|-----------------------------------|---------------------------|---------------|--------------------|
| ✓ | Roberto Giménez <i>ROBERTO</i> | H-Iberia | 4494856X | <i>[Signature]</i> |
| ✓ | Diego Fuentes <i>DIEGO</i> | H-Iberia | 51993960-E | <i>[Signature]</i> |
| ✓ | Emilio Martín <i>EMILIO</i> | H-Iberia | 52883624C | <i>[Signature]</i> |
| ✓ | Inma Luengo | H-Iberia | | |
| ✓ | Mario Carabano | Everis | | |
| ✓ | Sofía Virgos <i>CASAL</i> | Everis | 77445084M | <i>[Signature]</i> |
| ✓ | Jennifer Reina <i>GOÑEZ</i> | Everis | 11848288-E | <i>[Signature]</i> |
| ✓ | Sara Gutiérrez <i>ACIUEA</i> | Madrid City Council | 30722498E | <i>[Signature]</i> |
| ✓ | Fernando García <i>QUIZ</i> | Madrid City Council | 01917483-L | <i>[Signature]</i> |
| ✓ | Georgios Eftychidis | KEMEA | AE015348 | <i>[Signature]</i> |
| ✓ | Sophie Chague | Thales | 05PP82897 | |
| ✓ | Lucian Andrei <i>MIHAI</i> | MIRA TELECOM | DP137969 | |
| ✓ | Adrian Sima | MIRA TELECOM | 050210495 | |
| ✓ | Giorgos Kostopoulos | Aratos Technologies | AH1321113 | <i>[Signature]</i> |
| ✓ | Pedro António <i>EMMANUEL</i> | TEKEVER | 10976464 | |
| ✓ | Helena Granlund | FOI | 62386780 | <i>[Signature]</i> |
| ✓ | Anders Hansson | FOI | 56660927 | <i>[Signature]</i> |
| ✓ | Sami Ruponen | VTT | PR6327598 | <i>[Signature]</i> |
| ✓ | Timo Kytäjä | VTT | 190169-1115 | <i>[Signature]</i> |
| ✓ | Titta Ahola | VTT | 170675-0702 | <i>[Signature]</i> |
| ✓ | Peretz Burel <i>BUREL</i> | Athena | 9997598 | <i>[Signature]</i> |
| ✓ | Gaby Feldman | Athena | 23587340 | <i>[Signature]</i> |
| ✓ | Tassos Dimitriou | AIT | ABS644473 | <i>[Signature]</i> |
| ✓ | Sofia Tsekeridou | AIT | | |
| ✓ | Santiago Vilarino | M30 Madrid Command Centre | | |
| ✓ | Juan Carlos Díaz | M30 Madrid Command Centre | | |

| NAME | COMPANY | IDENTITY CARD | SIGNATURE |
|---|--|---------------|--------------------|
| Sarah Aubertin | INFINITY project | 091291300598 | <i>[Signature]</i> |
| Valentin Ifrim | Bucharest City Council | RO 7 18249 | <i>[Signature]</i> |
| Giorgos Kourelas | Grevena Civil Protection | AB951931S | <i>[Signature]</i> |
| Rickard Westning | Attunda Fire Department | 45591530 | <i>[Signature]</i> |
| Anssi Lehtinen | Helsinki City Council | PT0012191 | <i>[Signature]</i> |
| Jussi Koivisto | Helsinki Police Department | PK7782256 | <i>[Signature]</i> |
| Javier F. Martínez <i>de Guesada</i> | Madrid City Council | 00659649D | <i>[Signature]</i> |
| Elena de la Paz | Madrid City Council | | <i>[Signature]</i> |
| Carlos Rubio <i>Aguiar</i> | Madrid City Council | 00816403H | <i>[Signature]</i> |
| Gerardo Alonso | Madrid City Council | 5244089C | <i>[Signature]</i> |
| Rafael de la Gándara | Madrid City Council | 1110303A | <i>[Signature]</i> |
| V ^{to} Javier Ruiz Bertol | TECNALIA | 44977346H | <i>[Signature]</i> |
| ACHILLEAS | GREVENA CIVIL PROTECTOR KOURTELLAS | AB2072904 | <i>[Signature]</i> |
| ERNESTO GOMEZ GARCIA | AYUNTAMIENTO | 47065729-R | <i>[Signature]</i> |
| ROBERTO GAVASSI | TELECOM ITALIA | AO 00200021 | <i>[Signature]</i> |
| | | | |

5.5 Annex 5 – Invitation Letter

FP7-285556 SafeCity Project



Future Internet Applied to Public Safety in Smart Cities

Madrid, 22 July 2011

Dear Sir or Madam,

It is our pleasure to contact you regarding the European research project SafeCity (Future Internet Applied to Public Safety in Smart Cities). The motivation of the project is to enhance the role of the Future Internet in ensuring people feel safe in their surroundings at time that their surroundings are protected.

SafeCity aims at making Public Safety infrastructures smarter through tighter integration with Internet networking and computing capabilities.

SafeCity framework is envisaged to help Public Safety organizations collecting, sharing and analyzing data more effectively in order to make smarter real time decisions while planning and responding from incidents and emergencies. It will be split in four main areas depending on their functionality Situational Awareness, Ad-hoc Networks, Alerting Citizens and Command Centre technologies.

The objective of this workshop is to complete necessary information for SafeCity scenarios characterization, present the collected information in previous interviews, and to share last opinions among all Advisory Board, End Users and technical developers from consortium to elaborate a complete and appropriate Cities Scenarios definition and complete technical and functional requirements previously gathered.

It is therefore our pleasure to hereby cordially invite you to participate in the SafeCity Scenarios Workshop, which will be held at Isdefe premises in Madrid (Spain) on September 6th, hosted by the SafeCity project team.

In order for us to proceed with the arrangements we need your confirmation as soon as possible and it would be necessary you to provide us with contact data (full name, position in your company, email or telephone number), of the person/s who will attend by the 30 August 2011 the latest.

I truly believe your participation could be beneficial both for yourself and us, and I hope to see you in Madrid.

Please don't hesitate to contact me if you have any questions, or require further information.

Yours faithfully,

Diego Giménez Pérez
Sistemas de Defensa y Seguridad
Tel. +34 91 271 12 68
Mobile. +34 639 852 268
email: dgimenez@isdefe.es

© SafeCity Consortium

1

