FP7-285556 SafeCity Project

Deliverable D5.1

Experimentation Plan

Deliverable Type:	**PP**
Nature of the Deliverable:	**R**
Date:	**11/04/2013**
Distribution:	**WP5**
Editors:	**HI-IBERIA**
Contributors:	**ISD, AIT, ARA, MIT, VTT, EVE, FOI, TEN**

***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 contains the experimentation plan to be developed in the following 2 years.

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
HI-IBERIA	Diego Fuentes, Roberto Giménez
ISDEFE	Diego Giménez, Pilar Campos
EVERIS	Mario Carabaño, Sofía Virgos
AIT	Sofia Tsekeridou
TECNALIA	Estibaliz Delgado, Alejandro Villamarin
FOI	Anders Hansson, Jiri Trnka
MIRA TELECOM	Bogdan Curculescu
ARATOS	Giorgos Kostopoulos
VTT	Titta Ahola

Document History

Date	Version	Editor	Change	Status
20121220	0.1	Diego Fuentes, Roberto Giménez	First draft version of D5.1: Deliverable Template	Draft
20130225	0.2	Diego Fuentes, Roberto Giménez	Second draft version of D5.1, including contributions from ISDEFE and EVERIS	Draft
20130315	0.3	Anders Hansson, Jiri Trnka	Contribution to Section 5	Draft
20130315	0.3	Bogdan Curculescu	Contribution to Sections 5 and 6	Draft
20130320	0.3	Estíbaliz Delgado, Alejandro Villamarín	Contribution to Section 5	Draft
20130321	0.3	Sofia Tsekeridou	Contribution to Section 4	Draft
20130402	1.0	Diego Fuentes, Roberto Giménez	Final version of D5.1 ready for internal review. Contributions from all partners integrated	Draft
20130411	1.1	Diego Fuentes, Roberto Giménez, Diego Giménez, Sofia Tsekeridou	Final version of D5.1 after internal review	M24 Official version

Table of Contents

List of Authors iii
Document History iv
Table of Contents v
List of Figures viii
List of Tables ix
Glossary x
References xi
1. Introduction 1
1.1 Scope and objectives 1
1.2 Deliverable structure 1
2. Intellectual Property Rights issues 2
2.1 Intellectual Property Rights related to Phase 1 SafeCity Foreground 2
2.2 Intellectual Property Rights related to Background needed for using Phase 1 SafeCity Foreground 3
2.3 Intellectual Property Rights related to Foreground generated by other Use Cases 3
3. Plan for User Community Building 5
3.1 Cities community Group 6
3.2 Citizens Community Group 7
3.3 Industrial Community Group 8
4. Definitions of R&D technologies for Phase 2 11
4.1 SafeCity Phase 2 Research and Technology Vision vs. the defined Phase 2 Case Studies 11
4.2 Phase 2 Applications: Functional Description and Specific and Generic enablers 13
4.2.1 APP1 - Sensors Activation, Control & Information Enablement 14
4.2.2 APP2 - Heterogeneous Data Aggregation and Preprocessing 14
4.2.3 APP3 - Scalable Multimedia Analytics and Multimodal Fusion 15
4.2.4 APP4 - Heterogeneous Data Streaming and Storage 18
4.2.5 APP5 - High Level Data Fusion & Reasoning, Semantic Information Management 19
4.2.6 APP6 - Decision Support System for Action 21
4.2.7 APP7 - Communities Involvement & User Generated Content Management System 25
4.2.8 APP8 - Communication and Data Security, Privacy and Control 27

4.2.9 APP9 - SafeCity Phase 2 Business Exploitation Platform (BEP) 29
4.2.10 APP10 - Performance Monitoring and Evaluation Tools 30
5. Characterization of potential infrastructures 32
5.1 Characterization of potential infrastructures according to SafeCity Global Framework 32
5.1.1 Potential infrastructures according to Madrid Framework Characterization 32
5.1.2 Potential infrastructures according to Stockholm Framework Characterization 36
5.1.3 Potential infrastructures according to Bucharest Framework Characterization 40
5.2 Characterization of INFINITY potential infrastructures 41
6. Test-bed pre-selection 46
6.1 Madrid Test-bed 46
6.1.1 Test site and motivation 46
6.1.2 Potential infrastructures to be used 47
6.1.3 Communities involved 47
6.1.4 Ethical and Legal Framework 47
6.2 Athens Test-bed 48
6.2.1 Test site and motivation 48
6.2.2 Potential infrastructures to be used 48
6.2.3 Communities involved 49
6.2.4 Ethical and Legal Framework 49
6.3 Turin Test-bed 49
6.3.1 Test site and motivation 49
6.3.2 Potential infrastructures to be used 50
6.3.3 Communities involved 50
6.3.4 Ethical and Legal Framework 50
6.4 Bucharest Test-bed 51
6.4.1 Test site and motivation 51
6.4.2 Potential infrastructures to be used 52
6.4.3 Communities involved 52
6.4.4 Ethical and Legal Framework 52
7. Definition of experimentation infrastructure for Phase 2 53
7.1 Phase 2 Case Studies 53
7.1.1 Case Study 1: Enhanced detection and tracking of a suspicious citizen 53

7.1.2 Case Study 2: Early detection of a suspicious abandoned backpack in a public space and subsequent evacuation order 55
7.1.3 Case Study 3: Early detection and response for critical changes in road condition 56
7.1.4 Case Study 4: Early detection of an environmental incident 57
7.1.5 Case Study 5: Intelligent and trustworthy management of large events 58
7.2 Test Definition 60
7.2.1 Madrid Test-bed 60
7.2.2 Athens Test-bed 60
7.2.3 Turin Test-bed 60
7.2.4 Bucharest Test-bed 61
8. Assessment of Phase 2 success 62
8.1 SafeCity belonging FI-PPP: 63
8.2 SafeCity start-up: 64

List of Figures

Figure 1 EoI in further stages of SafeCity 6
Figure 2 Process to build the Industrial Community Group 8
Figure 3 SafeCity Phase 2 High Level Architecture 11
Figure 4 SafeCity Phase 2 Envisioned Technology Components and their Interaction 13
Figure 3 Google Earth image of AZCA 46
Figure 4 Crossroad in Patision with Solomou Street 48
Figure 5 Key areas of interest: the park near *Mercadante* Street (left), the open air market in *Foroni* Square (centre) and the main streets in *Barriera di Milano* zone (right). 50
Figure 6 *Obot Market* Area for Trial 51
Figure 13 Possibilities to achieve the success of SafeCity concept in Phase 2 62
Figure 14 Involvement of end users and SME's and Communities Group 63
Figure 15 Business & Exploitation Model Map 64
Figure 16 SafeCity evolution after the end of the project 65
Figure 17 Different alternatives proposed by SafeCity in the Phase 2 of the project 67

List of Tables

Table 1 SafeCity Phase 2 Envisioned Applications 12

Table 2 Recommended potential infrastructures' metrics according to Madrid Framework Characterization 36

Table 3 Recommended potential infrastructures' metrics according to Stockholm Framework Characterization. 39

Table 4 Recommended potential infrastructures' metrics according to Stockholm Framework Characterization. 41

Table 5 Applications involved in Phase 2 Case Study 1 55

Table 6 Applications involved in Phase 2 Case Study 2 56

Table 7 Applications involved in Phase 2 Case Study 3 57

Table 8 Applications involved in Phase 2 Case Study 4 58

Table 9 Applications involved in Phase 2 Case Study 5 60

Glossary

Acronym	Meaning
ADSL	Asymmetric Digital Subscriber Line
APP	Application
BEP	Business Exploitation Plan
C2	Command & Control
CCTV	Closed-Circuit Television
DSL	Digital Subscriber Line
EoI	Expression of Interest
EU	European Union
FTTH	Fiber To The Home
GE	Generic Enabler
GPRS	General Packet Radio Service
GSM	Global System for Mobile
HSDPA	High Speed Downlink Packet Access
ICT	Information and Communications Technology
IoT	Internet of Things
IPR	Intellectual Property Rights
LAN	Local Area Network
LTE	Long Term Evolution
OD	Operational Domain
PEST	Political, Economic, Social and Technological
PLC	Power Line Carrier
PoC	Proof of Concept
QoE	Quality of Experience
QoS	Quality of Service
R&D	Research & Development
SC	SafeCity
SC2	SafeCity Phase 2
SE	Specific Enabler
SWOT	Strengths, Weaknesses, Opportunities and Threats
VDSL	Very-high-bit-rate Digital Subscriber Line
WAN	Wide Area Network
XiPi	INFINITY Infrastructure website

References

Number	Reference
[1]	SafeCity Deliverable D3.2 Global SafeCity Framework Characterization
[2]	SafeCity Deliverable D3.3 Madrid SafeCity Framework Characterization
[3]	SafeCity Deliverable D3.4 Bucharest SafeCity Framework Characterization
[4]	SafeCity Deliverable D3.5 Stockholm SafeCity Framework Characterization
[5]	SafeCity Deliverable D6.2 Interactions with INFINITY Project
[6]	SafeCity Consortium Agreement
[7]	FI-PPP Collaboration Agreement

1. Introduction

1.1 Scope and objectives

The current document is associated to the task T5.1 - Experimentation Plan and presents the experimentation plan to be developed during the following two years. From the work performed in the tasks T2.1 - Public Safety Scenarios, T3.1 - Requirements Definition, T4.1 - Conceptual prototypes and T6.2 - Link with Objective 1.9, this deliverable will define and prepare Phase 2 of SafeCity.

This task works closely with the INFINITY and Core Platform FI-PPP projects. Although formally starting in M18, SafeCity consortium has previously, through T6.2 extensively, contributed to INFINITY database, so that those infrastructures and cities with high potentiality (and interest) for the realization of the whole SafeCity concept have been already included in the database and all its capacities, usage characteristics and authorities involvement are already reflected.

The idea of this deliverable is to start working in the next step of SafeCity vision at early stage, and thereby, the SafeCity Consortium is fully prepared and with a clear vision of work to carry out in Phase 2.

1.2 Deliverable structure

The whole document goes around the following idea: preparation for Phase 2 of SafeCity.

Section 2 collects those IPR from partners or other Use Cases that could be essential for SafeCity and guarantee that, accordingly to Special Clause 41 and FI-PPP Collaboration Agreement, IPR is safely kept and available in case of need during Phase 2.

Section 3 presents the plan to be followed in order to build a user community.

Section 4 defines R&D technologies to be developed during Phase 2, taking into account the current state of conceptual prototypes and needs for the full realization of SafeCity framework.

Section 5 shows the characterization of potential infrastructures according to SafeCity global framework performing an extensive review of XiPi repository and evaluating the most interesting infrastructures for SafeCity Phase 2 and its potential cost/willingness.

Section 6 carries out the test-bed pre-selection for Phase 2 aligning/introducing new inputs to XiPi repository and coordinating new requirements/information from sites with INFINITY.

Section 7 defines the experimentation infrastructure to develop in Phase 2 both from initial cities considered in Phase 1 (T3.2) and from the new ones (from INFINITY database) with the aim of looking for large impact across Europe.

Finally, section 8 performs an objective assessment of the potential success of SafeCity concept in Phase 2.

2. Intellectual Property Rights issues

The *Intellectual Property Rights* or *IPR* definition says: "Patent, patent applications and other statutory rights in inventions; copyrights (including without limitation copyrights in Software); registered design rights, applications for registered design rights, unregistered design rights and other statutory rights in designs; and other similar or equivalent forms of statutory protection, wherever in the world arising or available; but excluding rights in Confidential Information or trade secrets".

This section aims to identify those IPR from partners or other Use Cases that could be essential for SafeCity and guarantee that IPR are safely kept and available in case of need during Phase 2, accordingly to SafeCity Consortium Agreement, Special Clause 41 defined in the Grant Agreement and FI-PPP Collaboration Agreement.

With the aim of identifying those IPR issues more easily, the identified IPR will be split in:

- Intellectual Property Rights related to Phase 1 SafeCity Foreground;
- Intellectual Property Rights related to Background needed for using Phase 1 SafeCity Foreground;
- Intellectual Property Rights related to Foreground generated by other Use Cases.

2.1 Intellectual Property Rights related to Phase 1 SafeCity Foreground

The *Foreground* definition says: "The tangible and intangible results which are generated under the project, including pieces of information, materials and knowledge and whether or not they can be protected. It includes intellectual property rights (e.g. copyrights, industrial designs, patents, plant variety rights), similar forms of protection (e.g. rights for databases) and know how or trade secrets (e.g. confidential information)".

Therefore, it can be considered that Phase 1 SafeCity Foreground is made up of:

- Official SafeCity Deliverables
- Phase 1 SafeCity Applications
    - Application 1 – Generating situation Insight based on Video Analytics
    - Application 2 – Ad-hoc network for sensor communication
    - Application 3 – Intelligent Sensors and Info Pre-Processing
    - Application 4 – Real-time positioning based on video-analytics and artificial intelligence for decision support
    - Application 5 – Data Fusion
    - Application 6 – Communication Security
    - Application 7 – Decision Support
    - Application 8 – Road track and Environment sensors
- Specific Enablers developed for Phase 1 SafeCity Applications by SafeCity partners.

In this case, the IPR related to this Phase 1 SafeCity Foreground are safely kept and available for SafeCity in case of need during Phase 2 thanks to the following articles agreed in the SafeCity Consortium Agreement:

- 6.4.4 Access Rights needed for carrying out the Project

  The second paragraph says: "The Parties agree that the Access Rights to the Foreground needed for carrying out the Project shall be granted on a royalty-free basis".

- 6.4.5 Access Rights needed for Use of a Party's own Foreground

  The Section 6.4.5.2 says: "The Parties agree that the Access Rights to the Foreground of another Party needed for Use of a Party's own Foreground shall be granted on a royalty-free basis for research and demonstration activities under the Future Internet PPP".

2.2 Intellectual Property Rights related to Background needed for using Phase 1 SafeCity Foreground

The *Background* definition says: "Information which is held by a Party prior to its accession to this agreement, as well as the intellectual property rights pertaining to such information, including the application that has been filed before its accession to this agreement, which is needed for carrying out the Project or for using Foreground".

Therefore, it can be considered that Background needed for using Phase 1 SafeCity Foreground is made up of the Background identified and listed by the SafeCity partners in the Annex C - List of Background:

- Background 1 - Movie Violence and Associated Multimedia Ontologies (AIT)
- Background 2 - Semantic-based video processing / analytics engine for violence clues detection in video data (AIT)
- Background 3 - Movie Violence Reasoning Engine (AIT)

In this case, the IPR related to this Background needed for using Phase 1 SafeCity Foreground are safely kept and available for SafeCity in case of need during Phase 2 thanks to the following article agreed in the SafeCity Consortium Agreement:

- 6.4.4 Access Rights needed for carrying out the Project

  The first paragraph says: "The Parties agree that the Access Rights to the Background needed for carrying out the Project shall be granted on a royalty-free basis".

- 6.4.5 Access Rights needed for Use of a Party's own Foreground

  The Section 6.4.5.1 says: "The Parties agree that the Access Rights to the Background of another Party needed for Use of a Party's own Foreground shall be granted on fair and reasonable conditions".

2.3 Intellectual Property Rights related to Foreground generated by other Use Cases

According the *Foreground* definition in the Section 2.1, it can be considered that Foreground generated by other Use Cases and needed by SafeCity for Phase 2 is made up of:

- Specific Enablers or other applications developed by other Use Cases and likely used by some of the Phase 2 SafeCity Applications.
- Generic Enablers developed by FI-WARE and used by some of the Phase 1 SafeCity Applications.

In this case, the IPR related to Foreground generated by Other Use Cases are safely kept and available for SafeCity in case of need during Phase 2 thanks to Special Clause 41 defined in the Grant Agreement and the following articles agreed in the FI-PPP Collaboration Agreement:

- 4.2.3.1. Access Rights to Complementary Foreground for Project Execution

  The Section 4.2.3.1 says: "Access Rights to Complementary Foreground Needed for the execution of any Complementary Grant Agreement are hereby requested in writing and are deemed granted on a royalty-free basis to and by all Parties for the sole purpose of the execution of the Complementary Grant Agreement and such Access Rights shall automatically cease when the corresponding FII Project has been executed".

- 4.2.3.2. Access Rights to Complementary Foreground for Use

  The Section 4.2.3.2 says: "Access Rights to Complementary Foreground Needed for Use of own FII Project Foreground shall be granted on fair, reasonable and non-discriminatory conditions to and by all Parties, solely for the Needed Use of own FII Project Foreground ...".

- 4.2.3.4. Access Rights to Generic Enablers and Generic Enablers Specifications

  Notwithstanding the Sections 4.2.3.1 to 4.2.3.3, the Section 4.2.3.4 says: "Access Rights to Complementary Foreground and Complementary Background included in Generic Enabler Specifications for the execution of any Complementary Grant Agreement and for Use and Access Rights to Complementary Background included in Generic Enablers which is Needed for the execution of the Complementary Grant Agreement are hereby requested in writing and are deemed granted on a royalty free basis to all Parties and by all Parties".

The generated foreground will be subjected in first hand to the FI-PPP Program provisions set up by the Commission in order to guarantee the maximum impact of the FI-PPP, the correct interoperability among all FI-PPP partners and the less administrative burden and as much as possible straight forward transfer of knowledge to interested third parties. During Phase 2, SafeCity will then negotiate common IPR issues with the rest of FI-PPP partners and Commission, so that a maximum sharing of information is achieved and IPR issues do not hinder collaboration.

3. Plan for User Community Building

The involvement of new actors, local and regional stakeholders within the FI-PPP program will be crucial for the future to ensure the large scale expansion of the platform usage, counting on a high number of new players contributing to the new developments but also users of the developed technology. SafeCity considers essential to start setting up the basis for the future and interact with interest parties and key actors in future stages. As part of this activity and in order to engage the participation of these different players in the Public safety field, SafeCity has envisaged the creation of different Communities with different roles to pave the path towards the future of SafeCity. In this context, several profiles have been considered creating different user communities: **City Community Group**, **Citizens Community Group** and **Industrial Community Group**, explained below. The objective of these groups would be to initiate collaboration with them and start exchanging information and fostering discussion both sides, SafeCity about the initiatives in the safety-related development and program progress and future actors to expose their impressions and ideas for future developments or even to start their own safety-related functionalities with the support of SafeCity and the rest of the community members.

It is essential when creating a community to publicize the existence of such community. Hence, as part of the community building, it was published a *Request for Expression of Interest* in several web-sites as SafeCity and Ideal-ist[1]. Ideal-ist is an international ICT partner search network, with more than 85.000 contacts in line with the international cooperation strategy of the European Commission. Today the Ideal-ist network consists of 70 ICT national partners from EU and Non-EU Countries, such as Associated States, Eastern European Partner Countries (EEPC) and Mediterranean Partner Countries (MPC) and emerging countries like China, Brazil, India, and South Africa in line with the international cooperation strategy of the European Commission.

[1] http://www.ideal-ist.eu/

Figure 1 EoI in further stages of SafeCity

The objective was to get the involvement of different entities in the future of SafeCity, thus what was requested was interested parties playing different roles according to the created Communities as Users of the concept, Industries, SMEs and other professionals interested in developing safety and security related applications, but also different cities and public representatives to give feedback in order to help to pave future developments to be tailored to users' needs. As part of future activities, it is expected to dispose of several tools to promote communities, implementing the actions necessary to engage new actors to the existing communities through the appropriate dissemination activities but also the suitable platform community to bring together organizations and individuals interested in the topic.

3.1 Cities community Group

SafeCity considers Cities authorities' support essential for the success of the whole program and a special key player to promote the effective uptake of smart standardized infrastructure in the Public Safety field as well as in other sectors. For that reason, it is considered important to create this group where these players are participants and part of the project.

SafeCity has already counted with collaboration of several public safety and authorities during the phase 1. 6 different cities representatives have been involved during the project helping the consortium to carry out the research activities. However, it is highly valuable to count on other cities' feedback that complements the activities performed and makes future research suitable for different cities' profiles, e.g. size, location or needs. The members of this group will be able to participate and assess the outcomes of the research coming up with recommendations and directions to follow and establish close collaboration for the future making SafeCity solution extensible and suitable for different cities and optimize the benefits from the solutions to users. The objective is to set up bases for further cooperation in next stages and at the same time SafeCity and FI-PPP program achievements are disseminated along most likely future players, paving the way to ambitious interconnected trials making more extensive usage of the Core Platform capabilities within future phases and beyond Phase 3.

Apart from the current cities that have collaborated during the first phase, there are several cities that have shown interest in taking part of future stages of SafeCity:

City Councils

- Madrid - Spain
- Turin - Italy
- Bucharest Sector 2 - Romania
- Tartu - Estonia
- Avila - Spain
- Sabadell – Spain
- Chisinau City Mayor – Republic of Moldava

Police departments

- Malaga - Spain
- Valencia – Spain

And Athens, with the support of its Athens Management Control Center, as well as the Science and technology agency of Bahía Blanca (Argentina).

3.2 Citizens Community Group

Citizens could act as valid and very useful sources of surveillance/emergency timely information to public safety authorities at the same time they get easier access to safety-related information. Hence, inclusion of citizens in the public safety field is essential to activate this information flow, by means of applications for participatory input and personalized safety alerts among other, as Safety-orientated applets installed on citizens or safety personnel's smart mobile devices to enable the two information flow directions: system-to user (public safety alert via push notifications) and user-to-system (user-generated reports of witnessed unsafe situations going to the authorities in charge of guaranteeing).

This would increase the role of the citizens themselves but also would help them to perceive the technology as a tool to help them rather than to control them.

Depending on the city, area, etc. there are already several resident and commercial associations willing to have safety and security mechanisms in their areas due to the existing security problems. For instance, in Azca, district of Madrid with nightlife problems, several associations have claimed for security measures. Comunazca, which is the Association of neighborhood-community presidents of Orense/Azca St., the Azca Businessman and traders association or the "Asociación La Viña" which represents the Community of Madrid Hotel Business Association, or in the Turin degraded area of Barriera di Milano, the citizens are willing to have this sort of applications having identified the UPTU[2]. These players are to be included in all the cities. Generally, in the majority of cities, graduates are willing to use innovative applications hence it is a target group to be included in this community.

3.3 Industrial Community Group

SMEs and Industrial groups are cornerstone for FI-PPP and SafeCity, especially for further developments, therefore the inclusion of this community group is essential to start cooperation with them in order to set up the basis for future cooperation, interact with them starting collaboration to pave the future. This community group will act as seed for the development of new services and applications that would position SafeCity concept as a successful paradigm in Future Internet applicability. This group would consist on potential developers for future steps to be part of a development environment to be part of, represented by a platform aligned with FI-WARE core platform to boost the participation of the group members and other stakeholders, allowing them to develop and test Public Safety applications related to SafeCity. This environment would be also a collaborative space to build the community where the newbie beginner could asks questions to advanced, experts or intermediate profiles from the group to make a strong community around safety related applications based on cloud-based FIWARE capabilities. These stakeholders would be engaged during all Phase 2, and especially Industry community group is expected to become the accelerator for further stages.

Figure 2 Process to build the Industrial Community Group

[2] http://www.uptu.it

The table below summarizes the different entities which have shown interest in becoming part of SafeCity hence potential players of the Industrial Community Group.

SMEs

- Medotics – Switzerland
- LiveU – Israel
- Ambar Telecomunicaciones – Spain
- Enzenties Tecnología Madrid – Spain
- XLAB – Slovenia
- VirtualWare Group – Spain
- Vaelsys – Spain
- Balmart – Spain
- Safecity – The Netherlands
- Codelse – Spain
- GeoActio – Spain
- Geographica – Spain
- ES Solutions – Italy
- Future Intelligence Ltd - Greece
- iSPIRAL – Cyprus
- Ixion – Spain
- Coöperstie DevLab – Spain
- BK Telematics
- Abada Servicios Desarrollo – Spain

Large Industries

- Intracom – Greece
- Deloitte Abogados y asesores tributarios – Spain
- Oberthur – France
- IBM – Belgium
- Sice – Spain

- Tempos21/ATOS – Spain
- Ayesa Tecnología. Sadiel – Spain
- GMV – Spain
- Alcatel Lucent

Universities & Research Centres

- Kingston University – United Kingdom
- University of Ulster – United Kingdom
- Ideko – Spain
- Universitat Politècnica de València - Spain
- Faculty of Electrial Engineering Bosnia and Hezergovina East Sarajevo – Sarajevo
- University of La Laguna – Spain
- University of Zilina – Slovakia
- Instituto Tecnológico de Aragón – Spain
- University of Barcelona and the Computer Vision Center of Catalonia – Spain
- University of Cyprus – Cyprus
- Tekniker – Spain
- Research Group of Biometrics, Biosignals and Security (GB2S) - Universidad Politécnica de Madrid – Spain
- Fundación CARTIF – Spain
- PSIC – Public Security Innovation Center – The Netherlands

Others

- Individual/Enterpreneur – Ciprus
- RTD (CIMNE)+SME (CITHECSA)+ City Council (Barcelona) - Spain

4. Definitions of R&D technologies for Phase 2

4.1 SafeCity Phase 2 Research and Technology Vision vs. the defined Phase 2 Case Studies

SafeCity in Phase 2 will build upon the research results as well as the developed, integrated and tested applications of SafeCity Phase 1, investing on the gained know-how and experience through the interaction, integration and testing of a number of FI-WARE GEs and re-using, extending the capabilities of and introducing new Specific Enablers, currently lacking from FI-WARE, which are vital for the full implementation of the SafeCity Phase 2 Public Safety Case Studies, as reported in D3.2. From a technological and research point of view, the major sub-systems of the SafeCity Phase 2 solution, as shown in Figure 3, are:

- the Multi-sensor Surveillance and Situational Awareness System that Public safety authorities and cities will operate,
- the complementary User Generated Content Management and Service Provisioning System and the respective mobile applications to enable communities active involvement in public safety (professionals, citizens) and instant alert notification of the latter,
- the Business Exploitation Platform for Stakeholders such as SMEs to offer the means for full exploitation and re-use of SafeCity Phase 2 developed technology along with FI-WARE technology.

To this end, 10 core SafeCity Phase 2 Applications have been defined, re-using, extending and introducing new SafeCity Phase 1 Applications and Specific Enablers, in order to address all functions of the three major sub-systems of SafeCity Phase 2 and its envisioned Case Studies, on top of a significant number of FI-WARE GEs, presented in the sequel.

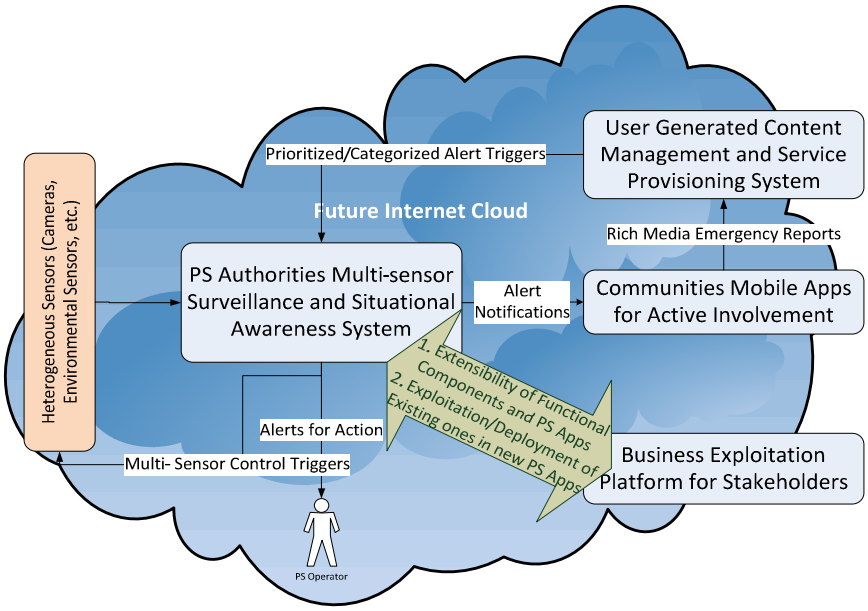


Figure 3 SafeCity Phase 2 High Level Architecture

Table 1 presents the complete list of defined Applications to be researched upon and developed in SafeCity Phase 2, completing its full lifecycle in Public Safety and facilitating large-scale scalable multi-sensor pilots. Each of them is based on a set of Generic and Specific Enablers, a number of which have

already been used and developed in SafeCity Phase 1, while the rest are envisioned to be developed in Phase 2. In the sequel, both the usage extent of FI-WARE Generic Enablers is presented as well as the brief description and function of the Specific Enablers in relation with each SafeCity Phase 2 Application.

APP Name	APP Description
APP1: Sensors Activation, Control and Information Enablement	Handles activation, configuration, connectivity and control of heterogeneous sensor devices (surveillance cameras, other types of sensors)
APP2: Heterogeneous Data Aggregation and Preprocessing	Tackles aggregation of data from heterogeneous data sources (sensors) in a synchronized manner, as well as undertakes feasible sensor data preprocessing in real-time at gateway devices located near the sensors.
APP3: Scalable Multimedia Analytics, Multimodal Fusion	Efficiently analyses in near real-time huge amounts of simultaneously streamed multimedia data (images, videos, audio, text) from camera sensors and citizens rich media emergency responses. Includes rich set of text, audio, image and video analysis and processing, pattern recognition algorithms to produce low and middle-level detection results, fed to multimodal fusion techniques to account both for higher accuracy in detection and higher semantics inference from single sources data processing
APP4: Heterogeneous Data Streaming and Storage	Provides core storage and distribution facilities in multimedia content and information workflows for other APPs and within higher level SafeCity Phase 2 Case Studies. It provides persistence and the associated query interface for heterogeneous content and metadata.
APP5: High Level Data Fusion & Reasoning, Semantic Information Management	Provides the semantic inference computational framework for public safety situation detection, based on decision level fusion of detected entities/events from multiple concurrent sources hinting the same incident, and on ontological reasoning to detect the semantic incident based on predefined public safety ontology. It further deals with the necessary semantic information storage and querying.
APP6: Decision Support System	Provides the core system for visually alerting public safety personnel on detected public safety incidents (from APP5) and assisting decisions for action (either manual by operators interacting with the given tools or automated). Among its functionalities, the following ones are included: decision support system, messaging/alerting, interactive UI, APP controls where required, 3D positioning and tracking.
APP7: Communities Involvement & UG Content Management System	Enables the involvement of communities in public safety (both professionals as well as volunteering citizens). Provides both mobile applications for public safety to actively involve communities, enable them to send rich media emergency messages and receive alert notifications, and the backend system for managing both communities and user generated content, the latter with respect to filtering, classification and prioritization according to the conveyed emergency message and user credibility.
APP8: Communication and Data Security, Privacy Control	Secures communications and ensures data privacy, at different levels of the SafeCity Phase 2 protocol stack, by finding the correct technologies and designing frameworks that mitigate attacks and thwart deviations from the implemented protocols to the greatest possible extent. Manages security aspects of all APPs. Further enables discrimination of security relevant data.
APP9: Business Exploitation Platform	Provides support for interaction with external third parties, especially SMEs and industry, by offering an easy-to-use system to evaluate the convenience of the deployment of a SafeCity Phase 2 public safety solution. Acts as tool to promote the more general FI-WARE platform by offering both technical- and business-minded access to its developments and GEs.
APP10: Performance Monitoring and Evaluation Tools	Provides performance monitoring and evaluation tools for SafeCity Phase 2 trials in order to objectively evaluate the performance of all APPs within the trialed public safety Phase 2 case studies. Includes data logging from each APP (SEs and GEs) for the defined performance criteria (response times, quality of service, false alarm rates, etc.), data analysis and mining to infer and visualize collective performance and spot cases of faulty operation or low performance in order to provide feedback to APPs to properly tackle and overcome such cases.

Table 1 SafeCity Phase 2 Envisioned Applications

The high level interaction of the defined APPs is shown in Figure 4. APPs 1-6 and 8 compose the SafeCity Phase 2 Public Safety Surveillance and Situational Awareness Sub-systems i), APP7 refers to the complementary User Generated Content Management and Service Provisioning Sub-System and mobile applications ii) for communities involvement, while APP9 corresponds to the Business Exploitation Platform Sub-system iii) of the high level SafeCity Phase 2 architecture. Finally, APP10 has been introduced to assist the automated performance evaluation of APPs under real-life deployment contexts and form the basis for such tools provisioning further to third parties and stakeholders to test their own SafeCity Phase 2 deployments.

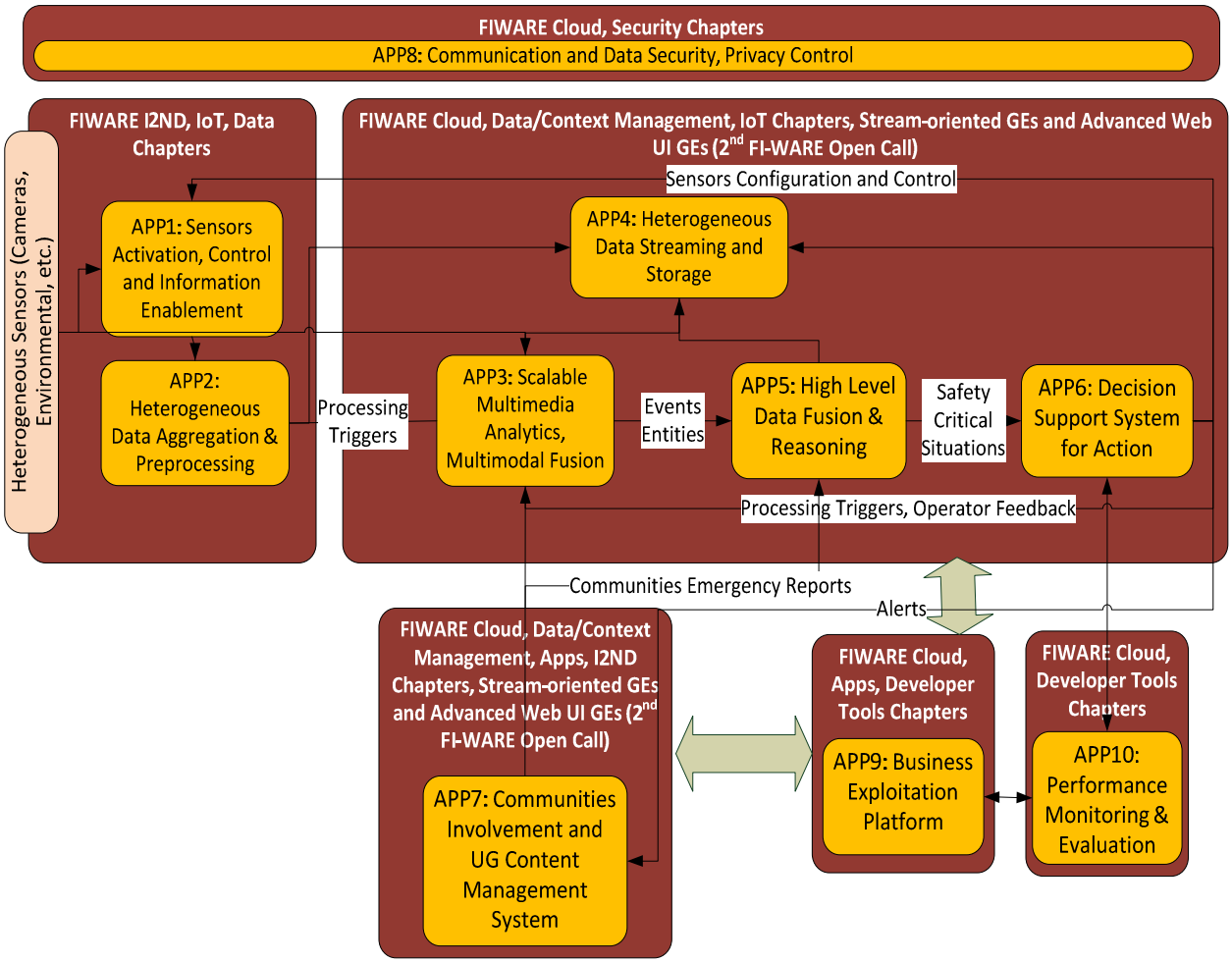


Figure 4 SafeCity Phase 2 Envisioned Technology Components and their Interaction

4.2 Phase 2 Applications: Functional Description and Specific and Generic enablers

The complete functional specification of the envisioned applications for SafeCity Phase 2 to facilitate the realization of the Phase 2 Case Studies is presented in the below presented table. For each APP, the description presents both Specific Enablers, re-used from Phase 1 and extended or newly introduced ones, as well as the inter-relation and utilization with FI-WARE GEs in the current or new releases of the latter.

4.2.1 APP1 - Sensors Activation, Control & Information Enablement

APP1 - Sensors Activation, Control & Information Enablement
SCOPE – SHORT DESCRIPTION OF FEATURES/CAPABILITIES
This technological component will handle the activation, configuration, connectivity and control of heterogeneous sensor devices such as surveillance video cameras as well as other types of deployed sensors, such as fire and smike detectors, road local weather and substance sensors, etc. that provide crucial data and information to enable situational awareness and thus promote safety and security. Among the main functions and capabilities of this APP lie the following: • Sensor interfacing (based on their APIs) and connectivity • Sensor device management, activation (e.g. while in "sleep" mode for energy efficiency), monitoring (battery level, normal operation, etc.), configuration and remote control • Multiple sensors management and information enablement (sensor data delivery) • On sensor data processing, for those sensors with such capabilities (e.g. cameras) **SEs** *Phase 1* *Serial Communication SE* Several sensors communicate through serial data interfaces, such as RS232 and RS485. The Serial Communication SE encapsulates common functionalities needed to access the serial ports. *ZigBee Communication SE* Similarly to Serial Communication SE that encapsulates common functionalities of communication through serial port, the ZigBee Communication SE encapsulates the common functionalities for ZigBee. *Sensor Frontend SE* Accounts for the interfacing, management and control of various types of sensors to be used in the project (camera sensors, environmental sensors, etc.), according to their communication protocol and API. In Phase I it only tackled road sensors interfacing *Phase 2* *On Sensor Data Processing SE* Accounts for the enablement of "smart" sensors, capable of on-sensor processing using their APIs and embedded software, for e.g. data pre-processing. **FIWARE GEs** *IoT.Gateway.Device Management GE* *IoT.Gateway.Protocol Adapter GE* *Publish / Subscribe Broker component of IoT.Gateway.DataHandling*

4.2.2 APP2 - Heterogeneous Data Aggregation and Preprocessing

APP2 - Heterogeneous Data Aggregation and Preprocessing
SCOPE – SHORT DESCRIPTION OF FEATURES/CAPABILITIES
This component specializes in assembling data from heterogeneous data sources (sensors) with different scores of uncertainties and trust and in a synchronized manner especially for data coming from co-located sensors but also for those coming from close proximity sensors. Then it performs the following tasks: 1. **Data pre-processing**: The purpose of this is pre-process received signals (noise removal, filtering) for subsequent processing. Additionally, this provides data selection and prioritization for further delivery (and storage) by APP4. At

this point simple light-weight analysis of the data will yield outliers, gaps, and flag important features for subsequent APPs. The preprocessing results are transformed to standard metadata formats (e.g. ONVIF for camera sensor data preprocessing results).

2. **Aggregating heterogeneous data:** It provides the ability to aggregate data from multiple data sources (sensors) referring and interfacing with APP1 and its Sensor Frontend SEs. This process is performed via computationally inexpensive synchronization and sensor sequence alignment methods.

SEs

Phase 1

Gateway Manager SE (including sub-components Data Integration SE, Data Processing SE and Data Management and Priorization SE)

- Base the initial data aggregation and pre-processing of the APP in the results of the Phase 1 SafeCity specific SEs. Re-distribute the functionalities and components into the extended and new SEs. Extend the capabilities to accommodate new sources of data in SafeCity Phase 2.

Phase 2

Sensor Data Preprocessing SE

- To provide the main data preprocessing capabilities in the APP: data clean up, conversion of metadata formats, data gateway interoperability for the different operational domains, securing of incoming data, basic management of scalability. Includes light-weight heterogeneous data preprocessing algorithms (for various types of sensors) to coarsely analyze and filter out most relevant such data with primitive hints for potential "abnormal" events (e.g. sensor data thresholding, camera data activity detection, etc.) that are transmitted in the form of metadata on the cloud, forming triggers for further advanced near real-time processing there.

Sensor Data Aggregation SE

- This SE will provide additional, higher-level pre-processing capabilities to the APP. Here basic data synchronization and alignment will be carried out.

FIWARE GEs

Data.Metadata Preprocessing GE

Data.Compressed Domain Video Analytics GE

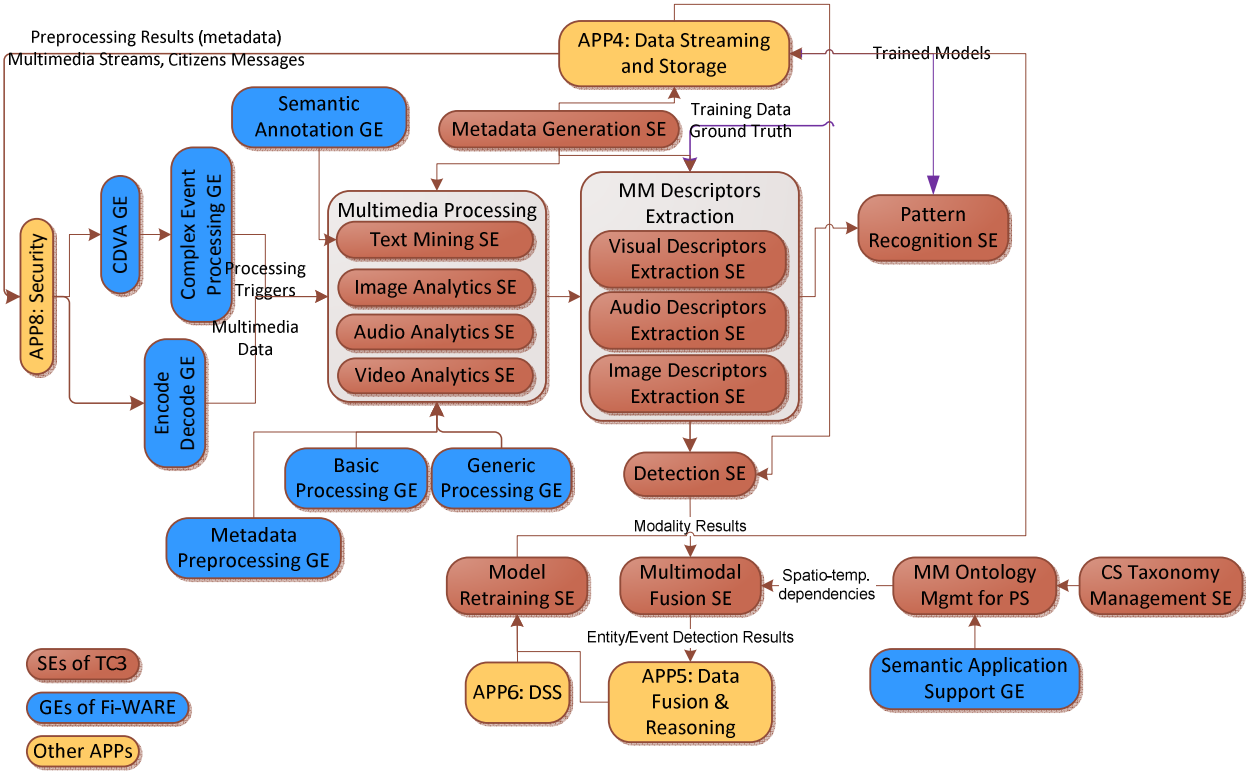
IoT.Gateway.Device Management GE, IoT.Gateway.Data Handling GE and IoT.Gateway.Protocol Adapter GE

4.2.3 APP3 - Scalable Multimedia Analytics and Multimodal Fusion

APP3 - Scalable Multimedia Analytics and Multimodal Fusion
SCOPE – SHORT DESCRIPTION OF FEATURES/CAPABILITIES
The purpose of APP3 is to efficiently analyze huge amounts of simultaneously streamed and/or recorded and delivered multimedia data, mainly images and videos, but also audio from acoustic sensors or citizens data and accompanying text, either captured from city surveillance cameras and effectively analyzed to accommodate enhanced situational awareness, early detection of emergency and response, or sent by citizens through their mobile devices, reporting emergency cases. A rich set of text, audio, image and video analysis and processing tasks, as well as pattern recognition and machine learning algorithms will produce low and middle-level detection results such as activity detection, background modelling and subtraction, background change detection, illumination normalization, person/vehicle or other moving object detection and tracking, face detection and recognition, intrusion detection, orphan object detection, person tracking, movement pattern analysis, "abnormal" person movement pattern detection (loitering, falling, fighting, running, stealing, etc.), object of interest segmentation and identification (weapon, person, car), car accident detection, illegal parking detection, crash sound detection, etc. Such low- or middle-level multimedia analysis results stemming from single or close located multiple cameras, as well as citizens mobile devices will be encapsulated in the form of ONVIF-compliant metadata. Multimodal fusion algorithms will further be devised and deployed to account for inter-dependencies among concurrent and/or sequential detected events/entities in single modalities or sensor sources and thus allow a better understanding of the evolving safety situation within the multimedia data.

These will mainly focus on decision level fusion/fusion of detection results from single modalities or concurrently transmitting sensor sources to account both for higher accuracy in detection and higher semantics infering in single sources data processing. It will be facilitated at an extent by Multimedia Ontologies for Public Safety, coupled with the higher semantically defined Public Safety Domain Ontology in APP5.

High Level Architecture Diagram



SEs

Phase 1

Video Analytics SE

It will extend the Phase 1 respective SE by further incorporating a richer set of video analytics algorithms, more robust and high performant to account for a larger set of seeked objects/events/entities, real-life contexts (low illumination, low quality, outdoor settings, etc.). It operates in the spatio-temporal uncompressed domain.

Pattern Recognition SE

A rich set of machine learning/pattern recognition algorithms will be considered as extensions to its Phase 1 coutnerpart per envisioned public safety Case Study, sometimes further combining multiple classifiers to increase the accuracy of modeling and thus subsequent detection. Extensions will include further the tackling of other multimedia data such as audio.

Visual Descriptors Extraction SE

It will extend the Phase 1 respective SE to account for a variety of representative visual features for face/person/car/object /movement unique representation and form the input to the extended versions of Pattern Recognition, Detection and Model Retraining SEs, according to the entity/object/event visual modeling/clustering needs.

Detection SE

Its Phase 1 functionalities will be further extended to account for the detection phase of all considered in the extended PR SE classification and clustering algorithms. Extensions will include further the tackling of other multimedia data such as audio.

Model Retraining SE

This Phase 1 SE will be fully developed in Phase 2 for re-training and re-clustering purposes, based on newly incoming data that will be used as training/clustering data as the required ground truth will result from operators feedback (APP6). Its utmost purpose is to lead to optimal models/clusters of visually learned/detected entities/objects/events, and thus lead to better

detection performance in these cases.

Critical Situations Taxonomy Management SE

This Phase 1 SE will be extended in Phase 2 and largely complemented by the Phase 2 SE: Multimedia Ontology Management for Public Safety SE

Phase 2

Audio Analytics SE

This SE will analyze the data coming from audio/acoustic sensors (e.g. the ones provisioned for in the Athens trial scenarios – traffic safety). The processes to be conducted are noise filtering, audio change detection, audio segmentation, etc.

Image Analytics SE

This SE will provide image analytics including image enhancement and noise filtering, spatial segmentation, spatial region/object detection, object identification, image thresholding, etc. especially for images contributed by citizens, etc. in the spatial (uncompressed) domain

Text Mining SE

This SE will deal with text mining of citizens contributed rich media messages, parts of which will be textual content. The analysis will involve mainly the spotting of "critical" words (included in the taxonomy per safety scenario) and the interpretation of the semantics of the emergency report, for the English language.

Image Descriptors Extraction SE

This SE will focus on spatial image features extraction, such as shape, color, texture, size, etc. features to spatially represent objects/entities of interest e.g. a weapon or person based on shape, a face based on color, a car based on a combination of shape and size features, etc. for again the unique representation of these entities in order to formulate the necessary input to the extended versions of both Pattern Recognition, Detection and Model Retraining SEs, according to the entity/object/event visual spatial modeling/clustering needs.

Audio Descriptors Extraction SE

This SE will focus on audio descriptors extracted from acoustic signals as recorded by acoustic sensors. These acoustic features/descriptors such as trrasform coefficient, sound harmonics, pitch, audio intensity, duration, etc. will again formulate the inputs for the extended versions of Pattern Recognition, Detection and Model Retraining SEs, according to the entity/object/event auditory/acoustic modeling/clustering needs, such as sound classification and sound event detection.

Multimodal Fusion SE

This SE will account for multimodal data fusion algorithms to fuse (at the decision level, detection outputs) the detection results of multiple modalities or concurrent a/v sensors installed at the same location that "hint"/"detect" the same incident so as to improve the accuracy of the detected event or enable a higher semantic level infering of it. These algorithms will account for cross spatio-temporal dependencies among the multiple modalities (in rich media citizens messages such as text and image or video) or same location placed a/v sensors, as dictated further by the Multimedia (and temporal) formal ontologies, to enable the late fusion of detected results.

Multimedia Metadata Generation

All SEs that analyze and process multimedia data need to output results (detection results, multimedia features, etc.) in supported multimedia standards for data exchange interoperability purposes. This SE will manage the generation of such standardized metadata instances.

Multimedia Ontology Management for Public Safety SE

This SE will provide the mechanisms on top of the Semantic Application Support GE to define and manage multimedia ontologies in relation with the CS Taxonomy and Public safety – both spatial and temporal relations among multimedia primitives and hinted events/entities will be defined.

FIWARE GEs

Data.Compressed Domain Video Analysis (CDVA GE)

Data.Complex Event Processing (CEP) GE:

Data.Metadata Preprocessing GE:

Data.Semantic Application Support GE:

Data.Semantic Annotation GE:

Cloud. DCRM GE:

Stream-oriented GEs (2nd Call)

- Encode Decode GE
- Basic Processing GE
- Generic Processing GE

4.2.4 APP4 - Heterogeneous Data Streaming and Storage

APP4 - Heterogeneous Data Streaming and Storage

SCOPE – SHORT DESCRIPTION OF FEATURES/CAPABILITIES

This APP serves as the core component providing storage and distribution facilities in multimedia content and information workflows for other APPs and within higher level SafeCity Phase 2 Case Studies. It provides persistence and the associated query interface for heterogeneous contents including:

- images and video chunks acquired by CCTVs, users' mobile devices and other image/video capture devices
- data and information collected from sensors
- user generated (UG) information and contents (rich media messages)
- text and data retrieved from various sources (e.g. internet, legacy DBs/systems from PS authorities, etc.)
- geo-location information (for any of the above data types)
- data/information annotation, metadata, semantic tags from SafeCity Phase 2 "safety ontology" managed in APP5.

APP4 will support the handling and management of large volumes of data (big data), the provision of metadata- and semantic-based query and content retrieval as well as data (A/V) streaming to external applications (e.g. APP6 DSS for Action).

Secured data storage is ensured by interfacing with the services provided by APP8.

SEs

Phase 1

No SEs have been developed in Phase 1 covering APP4 functionalities.

Phase 2

Database Configuration and Management SE

This SE provides all base functionalities for the configuration and management of the different parts (data, multimedia, metadata/semantics) of APP4 contents storage capabilities. This includes also the definition and management of the information concerning contents access rights and policies (e.g. authorization and access restrictions for sensitive contents in relation to user categories) that are implemented and managed through APP8.

Data Storage, Query and Retrieval SE

This SE implements the data persistence and associated management functionalities for all kind of data and contents (except multimedia) processed by SafeCity Phase 2 APPs and Case Studies. This includes data acquired from sensors, generated by the users or produced by other SafeCity Phase 2 applications. Location and temporal relationships between data are also stored at this level.

Metadata Storage, Query and Retrieval SE

This SE covers all aspects related to the storage and management of metadata and semantics level information connected to all type of contents stored within APP4, including multimedia contents.

Data Delivery SE

Provides data search, retrieval and delivery across both data and multimedia storage SEs, through a query engine supporting metadata and semantic tags. Provides the query and data delivery interface of APP4 for all SafeCity Phase 2 APPs and Case Studies.

Multimedia Streaming SE

Provides MM data streaming (e.g. video streams) for other SafeCity Phase 2 APPs (e.g. APP6 DSS for Action) or Case Studies.

FIWARE GEs

Cloud.ObjectStorage GE

Data.BigData Analysis GE

Data.Semantic Application Support GE

Stream-oriented GEs (2nd Call)

- API GE
- Encode Decode GE
- Transport Protocols GE
- Management Monitoring GE
- Media Storage Retrieval GE

4.2.5 APP5 - High Level Data Fusion & Reasoning, Semantic Information Management

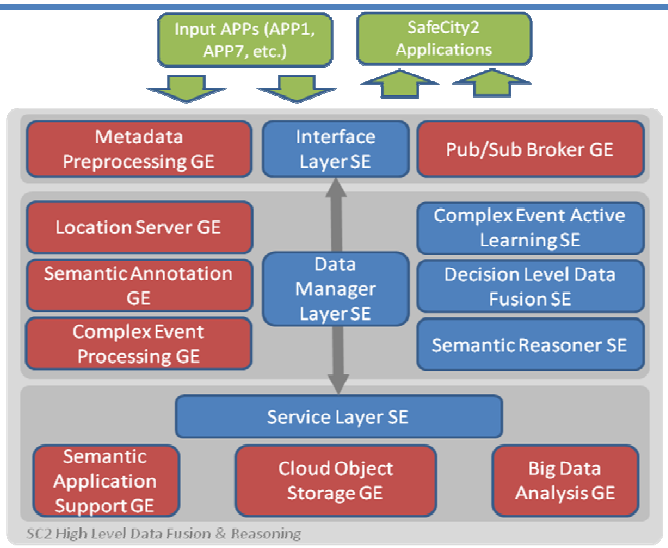
APP5 - High Level Data Fusion & Reasoning, Semantic Information Management

SCOPE – SHORT DESCRIPTION OF FEATURES/CAPABILITIES

This APP will be able to provide a computational framework for the modeling and storage management of data in the SafeCity Phase 2 system

- On the fly fusion of incoming data into higher level constructs defined by a consistent semantic model via a Public Safety ontology.
- Reasoning of complex events based on the fusion of the various sources, provide support for active learning of new events based on historical data.
- Provision of semantic information storage and querying system including interfaces to legacy systems at the data level via appropriate data and metadata bridges.
- Leveraging on concepts and technologies coming from different fields:
    - Semantics: ontologies to model the domains of interest, storage of captured metadata as RDF triples, SPARQL/SPARUL to query and update semantic data, C-SPARQL to provide on-the-fly reasoning, semi-automated annotation using Linked Open Data Sources.
    - Event detection and processing.
    - Semantic large data set crunching using Big Data (MapReduce) approaches.

High Level Architecture Diagram



SEs

Phase 1

Interface Layer SE

- Facilitates the provision of an API to interconnect the elements of the APP with the outside world (other elements in the SafeCity Phase 2 ecosystem and other knowledge sources). This is done using REST-based interfaces.
- The basic functionality will be extended to allow the usage of other interfacing mechanisms for external modules such as PubSub GE to allow subscribing to events. The Metadata PreProcessing GE will be integrated substituting ad-hoc solutions used in Phase I.

Data Management Layer SE

- Integrates the flows of information at the data understanding and management within the TC, providing communication pipelines between the different components of the module.
- Connect the baseline functionality with the Big Data GE in order to provide large scale data management capabilities.
- Leverage on the Semantic Annotation GE to connect with Linked Open Data sources for (semi) automatic annotation of inputs.
- Use the Location GE to provide automatic incorporation of location data to the semantic repository.

Service Layer SE

- Provide the semantic backbone of the TC and the basic data storage and querying features: an RDF triplestore which is accessible using a SPARQL/SPARUL API.
- Extensions during Phase II will include more controlled versioning of the ontologies using the SAS GE functionality.

PS Ontology

- Define the domain of Public Safety as used by SafeCity Phase 2; codify the needed concepts and their relationships in a formal language (RDF, OWL).
- These formal descriptions of elements will be used to build rules that fully use this semantic description and the Semantic Reasoner SE to extract new information of the domain or to provide detection of patterns.
- Provide means so that these rules can be automatically generated by the learning algorithms of the Complex Event Active Learning SE.

Phase 2

Complex Event Active Learning SE

- This specific enabler will integrate the needed functionality to enable machine learning algorithms to operate from the semantic data sets captured by the TC. It will provide a generic learning framework upon which several

strategies for machine learning may be connected.

Decision Level Data Fusion SE

- Offer late data fusion capabilities that unify at the semantic level the different streams of data incoming into the APP. It will provide several fusion mechanisms, from simple statistical ones (i.e., based on time sequences) to more advanced ones (i.e., incorporating the reasoning and machine learning elements of the APP)
- An internal module will be implemented for traffic analyzing using real-time streaming semantic data schema (e.g., traffic events from an intersection). It will use a sampling and filtering policy that will produce time stamped RDF triples (pairs <ρ, τ>. It will leverage on streaming SRARQL (C-SPARQL) or Time Annotated SRARQL (for static RDF graphs or transient streams of RDF triples) and on the integration of Statistical Sequential Event Detection Algorithms such as CUSUM for sequential event reasoning with optimized false alarm rate for crash event detection.

Semantic Reasoner SE

- This will build on top of the functionality offered by the SAS GE to provide a unified interface with which to implement several reasoning strategies that operate on the semantic data stored in the SAS repositories.

FIWARE GEs

Data.Complex Event Processing GE

Data.PubSub Broker GE

Data.LocationServer GE

Data.Metadata Preprocessing GE

Data.Semantic Annotation GE

Data.Semantic Application Support GE

Data.BigData Analysis GE

Cloud.Object Storage GE

4.2.6 APP6 - Decision Support System for Action

APP6 - Decision Support System for Action

SCOPE – SHORT DESCRIPTION OF FEATURES/CAPABILITIES

Decision Support System for Action (DSS) is intended to help decision makers to identify and solve problems, complete decision process tasks, and make decisions. Based on the resulted decisions, different actions can be performed. The purpose of DSS is to receive events/alerts, process the results according to the rules, present the proper information to the operator/decision maker and perform actions (automatically or manual).

The sub-components are the following:

- decision support system;
- sensors/processing triggers;
- messaging/alerting;
- GUI layout & interactive/intuitive UI;
- rule-based engine;
- 3D positioning and tracking;

Short description of each module:

DSS and Sensors/processing triggers

DSS makes the connection between several applications of APP6 and operator/decision/maker.

Depending on the scenario, an operator can define:

- different rules;
- automated responses to different events;
- triggers to sensors;
- alerting and messaging.

Messaging/alerting (incl. alerts on displays/information panels)

This module is in charge of informing citizens/authorities upon threats occurring in monitored areas.

GUI Layout and Interactive/Intuitive UI

Provides a common framework for all GUI software components. The layout must be user-friendly and provide capabilities like fly-out panes, floating windows, multiple docking manager in same window, styles and themes etc.

Furthermore, this module is in charge of the new user interface, intended to receive immediate feedback from the operator about any event that he/she sees on the screen. A touch screen will be used on which the operator can see both the video picture and also an overlay of intuitive sophisticated UI layer that will allow the operator to report immediately about any event.

Rule-based Engine

The rule-based engine uses data from the system metadata repository to reason about and make better inferences about the state of the system. For example:

- Detect reoccurring patterns of routine activity
- Detect irregular activity
- Detect deception attempts
- Detect correlation between observed events and external environment (holidays, planned large crowded events, weather conditions etc.)

3D positioning and tracking

Based on a 3D model of the pilot site, the technological component will offer a 3D view of the area, representing people in real time in the streets.

The 3D position of people will be extracted from multi-cameras video analytics. Based on an existing camera network and/or on deployed camera network, video analysis will extract people position in 3D.

Based on real life information coming from video analysis, a functionality of anticipation of people actions is developed. More precisely, two scales of behavior simulation will be proposed:

- The ability to predict the path when the field of view of the camera network does not cover the whole person path.
- The ability to trigger “What if scenarios” and simulate the behavior of people in case of specific events like fire, riots, etc...

SEs

Phase 1

DSS

*DSS Manager SE e*ncapsulates components for decision-making activities based on a knowledge system.

The Phase 1 SE will be **extended** with components that will be able to handle automated commands and triggers to different kind of sensors and with capabilities of defining messages and perform alerting/notifications based on specific defined scenarios Varying parameters (receiver, type of message, device capabilities etc.) are taken also into consideration. The manager can perform automated commands and triggers to different kind of sensors by invoking the Sensor Frontend SE.

3D real-time positioning

3D Display SE

The extension of this SE in Phase 2 is the scalability of the technology as well as the quality of the visualization which will

beneficiate of augmented reality features.

Tracks Management SE

The extension in Phase 2 of this SE is the scalability of the technology.

Single Tracker SE

The extension in Phase 2 will be the optimization of the use of CDVA GE as well as the management of a more large and complex area. The tracking of people will be more complex to manage in a mix indoor/outdoor area than in Phase 1. Also extended in order to track one pointed-out person from the multi-camera network.

Path prediction SE

. For phase 2, the prediction of people will be more complex to manage in a mix social area (mix of night club and business buildings) than in phase 1.

Behavior simulation SE

For phase 2, the simulation of people behavior will be more complex to handle in a mix social area (mix of night club and business buildings) than in phase 1.

Rules-based Engine (RUBE) SE composed of:

1. *Routine activity identification*

   allows the end user to understand if the event they see on the screen is a routine event, or not. This will be based on past history of the specific place, and the possibility for recurrence based on multiple temporal recurrences cycles (time of day, day of week, day of the year, holiday etc.).

2. *Exception handling*

   handles exception situations detected by the end user (or confirmed by the end user in response to detection by other means). This exception handling may include: Metadata storage, metadata retrieval, display of check lists of actions to perform, etc.

3. *Correlation with external environment*

   correlates specific events to the external environment. For example, if a big sport event is expected in a nearby stadium then large crowds of people are expected on the street at the time of the sport event. Knowledge about the sport event will be collected by the SE, instead of relying on the memory and general knowledge of the end user.

Phase 2

The following SEs will be developed:

Interactive/Intuitive UI

Interactive/Intuitive UI SE composed of:

1. *UI workflow*

   provides the optimal workflow of the end user. The workflow is dynamic and is a function of the events that are being handled by the end user at any given time, the specific function of the end user and the general alert level of the system as a whole.

2. *UI layout*

   decides on how to best lay the touch screen UI widgets (buttons, keys, alert signals, menus, check lists etc.) as a dynamic function of the picture viewed on the screen, the function of the end user and the general alert level of the system as a whole.

3. *UI interaction with other DSS modules*

   interfaces with the rest of the DSS (Decision Support System) modules in order to ensure smooth integrated operation of the DSS and the interactive/Intuitive UI as a coherent functional unit.

DSS - Sensor processing/triggers

Sensor Remote Configuration & Control Interface SE – defines the operations that enable users to remotely control sensors (like PTZ for a video camera); implements graphical user interface for remote sensor configuration, operation test and calibration (for city-installed video cameras); permits automatic management of sensors based on defined scenarios.

GUI Layout

GUI Framework SE is a common framework for presenting software GUI components to end user.

GIS Maps manager

GIS *Maps manager SE* integrates software, data for capturing, managing, analyzing, and displaying all forms of geographically referenced information. Allows end user to view, understand, question, interpret, and visualize data on a map.

Messaging/alerting

Alerts Messages Routing SE enables the routing of detected/inferred events/alerts from APP5 or operators interacting with APP6 GUI apps to the other APPs, to automatically control sensors, or to notify involved communities (on their mobile devices).

FIWARE GEs

DSS

Data.Publish/Subscribe Broker GE

Data.Complex Event Processing GE

Data.Big Data Analysis GE

Data.Location GE

Cloud. DCRM GE

GUI layout

Advanced UI of 2nd Open Call of Fiware

FIWARE.Epic.AdvUI.AdvWebUI.2D-UI

FIWARE.Epic.AdvUI.AdvWebUI.3D-UI

GIS Maps manager

FIWARE.Epic.AdvUI.AdvWebUI.GIS-Support

Sensors/processing triggers

IoT.Backend.Device Management GE

IoT.Gateway.Protocol Adapter GE

Data.Location GE

Sensors Remote Configuration & Control

IoT.Backend GEs

IoT.Gateway.Protocol Adapter GE

Real Virtual Interaction GE

2D User Interface GE

3D User Interface GE

Rule-based Engine (RUBE)

Data.CEP

Data.BigData

Data.PubSub

Data.MetadataPreprocessing

3D positioning and tracking

CDVA GE

CEP GE

Big Data GE

Advanced UI.Augmented Reality GE

Publish Subscriber GE

Cloud. DCRM GE

4.2.7 APP7 - Communities Involvement & User Generated Content Management System

APP7 - Communities Involvement & User Generated Content Management System

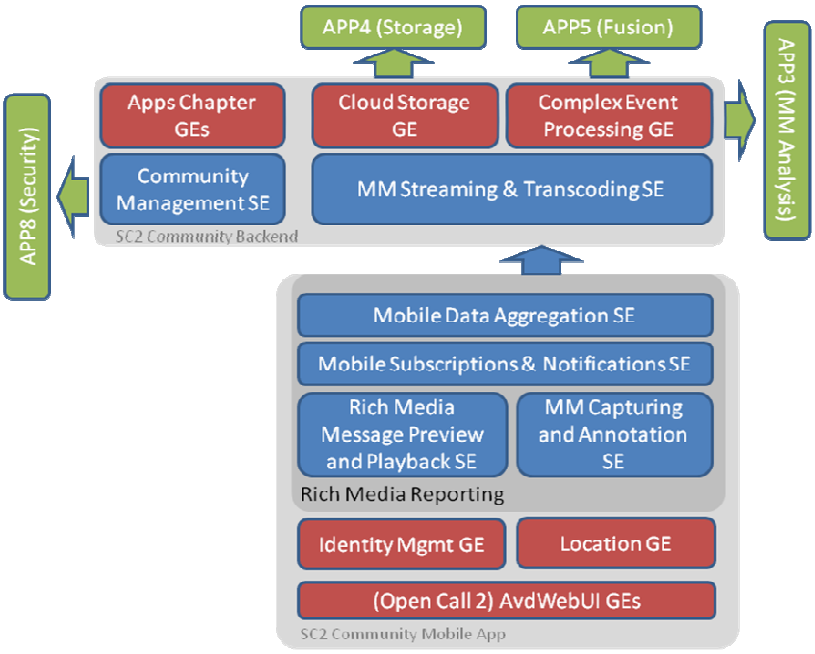
SCOPE – SHORT DESCRIPTION OF FEATURES/CAPABILITIES

This APP is a newly introduced one and will implement elements necessary for citizen-centered applications using SafeCity and FI-WARE components. This technology will help SafeCity study on the particulars of the involvement of ordinary end-users in the Public Safety information loop.

The application is geared towards integrating information provided by citizens in the form of rich media reports (e.g., including images/video plus text). For this, we will need to implement the following:

- A mobile front-end for mobile smart devices (iOS and Android) to provide two basic functionalities: users will be able to send input for the SafeCity Phase 2 processing systems (acting as citizen-sensors) and they will be able to subscribe to safety/security alerts provided by the SafeCity Phase 2 platform of their interest.
- The back-end that the mobile applications will connect to in order to send the captured data and to retrieve relevant data for the users.
- User community and profile management: user subscription, account management and depending on their profile (i.e. professional, citizen, etc) users will have access to a different set of functionalities, rights and available features.

High Level Architecture Diagram



SEs

Phase 2

Mobile Data Aggregation SE

Providing a unified transmission system to send rich media data from the user's mobile smart devices to the system backend and enabling the streaming front-end for the mobile device.

Mobile Subscription & Notifications SE

Context-/user-adaptable mobile application allowing users to subscribe to and receive location-relevant safety information (alerts, etc.).

Multimedia Capturing and Annotation SE

This SE will provide the content authoring and annotation functionalities to SC2 communities (professionals, citizens), within a component in the respective PS mobile application, for any type of public safety case study in SC2 to capture images/videos and author a rich media emergency message in quick, user-friendly and straightforward way, utilizing predefined rich media templates composed of graphics (safety symbols), textual placeholders for short textual messages, assisted by predefined emergency text messages. This SE will further build up the necessary intuitive 2D interactive UI components for such content authoring functionalities.

Rich Media Message Preview and Playback SE

This SE takes over after the Multimedia Capturing and Annotation SE has been invoked and a rich media emergency message has been authored, to allow the community member to preview and playback the result of the authoring process and then invoke the SEs for streaming/delivering the message. The processes involved are functionalities of a rich media player which will further allow for the re-authoring/editing of the message.

Mobile Multimedia Streaming and Transcoding SE

Based on the results of the Streaming Media Open Call in FI-WARE, will provide the means to do so from mobile devices, therefore enabling the sending of mobile video from the user's side to the processing algorithms in SafeCity Phase2's side.

Providing means to transcode the media to be sent by the mobile smart device to a format that is better suited for low-bandwidth situations.

Community Management SE

This SE will provide a centralized repository for the control of the community of users. This will keep track of their identities, activity and inputs and subscription to the notification system. In addition it will produce a trust and credibility profile for each user based on the quality of their contributions over time. The privacy of the stored data for users will be a fundamental design guideline for this component.

FIWARE GEs

Cloud.DCRM

Cloud.ObjectStorage GE

Data.Complex Event Processing GE

Apps.USDL GE

(Optionally) Apps.Repository GE, Apps.Marketplace GE, Apps.Registry GE, Apps.RSS GE and Apps.Mediator GE

Data.Publish Subscribe GE

I2ND.Connected Device Interface GE

Stream-oriented GEs – 2nd Open Call

- Encode Decode GE
- Transport Protocols GE

Results from the FI-WARE 2nd Open Call for Advanced UIs will also be explored, including but not limited to AdvWebUI.2D-UI (for the interactive UI components of Rich Media Message Preview and Playback, and Multimedia Capturing and Annotation

SEs), AdvWebUI.AdaptableUI (for tackling the cases of adapting the UI components of both SEs for different mobile devices) and AdvWebUI.2D-3DCapture (For providing the core mechanisms for image/video capturing on a mobile device)

4.2.8 APP8 - Communication and Data Security, Privacy and Control

APP8 - Communication and Data Security, Privacy and Control

SCOPE – SHORT DESCRIPTION OF FEATURES/CAPABILITIES

The integration of the physical world into the digital world is an important requirement for all Citizens and Traffic Public Safety case studies of SafeCity Phase 2, as an increasing number of services are relying on real world information. In this context, the communication network will be comprised of many heterogeneous devices such as sensors, actuators and tags that are all *networked* together. This highly dynamic and mobile setting presents new challenges for information security and personal data privacy, caused by the ubiquitous nature of produced data traces and the high volumes of trade and traffic that are pushing the boundaries of existing infrastructures and resources.

The goals of the Communication and Data Security, Privacy and Control application are to *secure communications* and *ensure data privacy*, at different levels of the SafeCity Phase 2 protocol stack, by finding the correct technologies and designing frameworks that mitigate attacks and thwart deviations from the implemented protocols to the greatest possible extent. It will enable the secure exchange of all network traffic regardless of sensor hardware and communication protocol heterogeneity, value range, precision or unit. Also, it will ensure the integrity of transmitted data since it addresses concerns related to confidentiality and preservation/retention of produced data. Furthermore, it will provide appropriate mechanisms which will ensure that the delivery and usage of services is not only trustworthy but meets certain security and privacy requirements. Key functionalities like identity management, secure storage and access control will be integrated in the design and implementation of the component platform. An overview of the areas covered by the above described application includes the following:

- **Security of Communications**: Protect the security of communicated data at the network level in the IoT domain.
- **Secure and reliable access to senor and actuator information services for multiple services.**
- **Identity and Privacy Management**: Trust relationship schemes for determining deployed node profiles that include their allowed set of actions and the force of their measured data/events.
- **Data Handling (including Data Destruction) and Secure Storage**: Focus on the privacy challenges associated with the handling and storage of personal data. Provision of appropriate mechanisms for controlling the usage of produced data traces; when the data is accessed by an application, and access technology control will be used to verify that the intended use of the data matches the scope defined by appropriate policies.
- **Prioritization of Public Safety broadband communications based on provided critical application data taxonomy**: Support different kind of network processing for the transmission of higher priority sensitive data/requests.
- **Confidentiality, Message authentication and Integrity, Entity authentication, Support of Trust and Group policies**.

SEs:

Phase 1

Below is a list of all the SEs that were introduced in Phase 1 of SafeCity project and will be also used and extended as part of the *Communication and Data Security, Privacy and Control* technical component (along with a brief description of the necessary extensions that have to be included):

Security Manager (SM) SE consisting of *Settings Configuration SE*, *Data Handling SE* and *Trust Management SE*.

This enabler encapsulates the security aspects of all envisioned applications and enforces the desired communication security policies. It is responsible for protecting network communications by defining the set of cryptographic transformations that have to be performed on the messages sent over the network. Possible list of extensions includes:

- Extend the SM's architecture to support the case studies envisioned by SafeCity Phase 2 in terms of immense scale of deployment and high level of heterogeneity; network model must support *mobility of nodes* and *addition* of new ones upon demand. Therefore, already integrated security solutions that assume fixed topologies cannot be employed.

- Support of different and "stronger" security policy sets (e.g., cipher suites, cryptographic protocols, etc.).
- Integration of all necessary security FI-WARE generic enablers that were part of the SM's architecture but were not released on time and, therefore, were removed in SafeCity Phase 1version.
- Optimization of the *authentication* and *authorization* mechanisms.
- Dynamic negotiation and possible update of all incorporated cryptographic primitives.
- Secure session and cache management.

Trust Management SE

This enabler is responsible for establishing *trust relationships* and managing *access lists* and *security profiles* among IoT devices/gateways. The main role is to verify that someone is who it claims to be and to determine if it is a legitimate part of the network.

- *The version of this SE was described in the context of SafeCity Phase 1 only for completeness*; it was not implemented since it was out of the official PoCs scope. Therefore, its architecture and functionality must be re-designed and implemented for the Citizens and Traffic Public Safety context.
- Specification, evaluation, establishment and assurance of trust relationships among IoT devices.
- Management of access and trust lists.
- Isolated identity management.
- Control stratification and impact sensitivity.

Phase 2

Below is a high level list of possible new specific enablers to be implemented during development:

Credential Manager SE for managing all necessary *credentials* and checking application requests that want to access provided services. It will deal with credentials or tokens that need to be provided to a user when accessing a requested service.

Actuator Location SE for being able to know *when* and *where* something was measured and/or happened. This also requires the use of clock synchronization mechanisms. Overall, in networks with mobile nodes it must be possible to localize a node relative to other nodes (used for building the trust relationships).*This SE will provide similar functionalities as the <FI-WARE>. <Localization Platform> GE but for a wide set of hardware devices; not limited to those that are equipped with a SIM card as is the case with the generic enabler.*

IoT Profile SE which will be responsible for determining the "*profile*" of each node in the network, the current device role, the current situation and context as well as maintain the security, privacy and trust association of each node.

Control Stratification SE for assuring that an entity handling, accessing and/or producing information (as part of an operation process), has the required privileges. The more sensitive the information is, the higher the requirement for the authentication result must be in order to be trusted.

Data Protection Manager SE which will be responsible for the implementation and administration of IT processes to ensure that recorded personal data is securely backed up, recovered and destroyed when necessary. Personal data profiles should not be retained for longer than needed to perform the task for which it was collected, or as required by laws and regulations. Such information (maximum allowed storage time, possible storage extension, etc.) will be provided by accompanying metadata that will be stored (along with the *actual* data), through appropriate interfaces, from APP4. It will consist of: *Data Retention & Processing SE*, *Metadata Management SE*, *Secure Data Destruction SE* and *Data Logging SE*.

Secure Storage SE for enabling a level-based security storage that will apply different levels of encryption to the stored information based on their sensitivity and importance. It will interface with APP4 storage functionality and will further optimize computation and communication traffic through the use of light cryptographic schemes when necessary. Furthermore, it will be tightly coupled with the <Security>. <Optional Security Enablers>. <Secure Storage Service> GE for providing accompanying read/wright access privileges in function of the identity of the authenticated requester.

FIWARE GEs:

All the above described SEs will develop interfaces and interoperable mechanisms to support the *secure communication* and

data privacy between distributed things and devices/gateways in cooperation with various underlying FI-WARE generic enablers. GEs upon which specific enablers will base their functionality are:

<Security>. <Security Monitoring> GE

<Security>. <Context-based Security & Compliance> GE

<Security>. <Identity Management> GE

<Security>. <Privacy> GE

<Security>. <Optional Security Enablers>. <Secure Storage Service> GE

<Security>. <Data Handling> GE

<Data>. <Location> GE

<Data>. <Metadata Preprocessing> GE

<Resources Management>. <Services & Resources>

4.2.9 APP9 - SafeCity Phase 2 Business Exploitation Platform (BEP)

APP9 - SafeCity Phase 2 Business Exploitation Platform (BEP)

SCOPE – SHORT DESCRIPTION OF FEATURES/CAPABILITIES

SC2 BEP's key objective is to provide support for interaction with external third parties and especially geared towards SMEs and industry. The Exploitation Platform will provide an easy-to-use system to evaluate the convenience of the deployment of a SafeCity Phase 2 solution. It will be also used as a tool to promote the more general FI-WARE platform as it will offer both technical- and business-minded access to its developments and GEs. Compliance with the FI-WARE technology (GEs and SEs will be offered and the API itself will be based on GEs and SEs where possible) and approach (production of reusable components) will be a key driver in the production of the platform.

The SC2 BEP will be composed of two key main modules that provide access to the platform at differing complexity levels:

BEP Workbench Access API

In line with the Future Internet development paradigm, this provides a technical bridge to the reusable functionalities offered by the SafeCity Phase 2 environment (case studies, APPs, SEs and GEs) by offering an API so that the higher-level oriented SC2 Exploitation Platform can connect to it and provide more technologically abstracted tools to build services and manage them from a business perspective.

SafeCity2 Exploitation Platform

In order to boost the participation of SC2 stakeholders that may not be as technically minded (SMEs, entrepreneurs, etc.) and taking into consideration some of the GE and advantages offered by FI-WARE core platform, the 'Exploitation Platform' will be designed as a low-barrier 'access point' for organizations and developers wishing to develop Public Safety applications related to SafeCity Phase 2. This 'access point' will let SC2 stakeholders find, understand and use the different SC2 Applications (APPs) and operational modules in an easy way. Moreover, in order to help non-advanced 'users' to develop their applications, all the SC2 components will be available as aggregated and categorized components in a simple market place with different features to support them. For those advanced users that require further detail access of the applications, the platform will give them access to that information if they are authorized.

The 'Exploitation Platform' will be also designed as a fully functional platform connected to SC2 APPs. Therefore, it will have its own administration module (the Platform Manager SE).

Developers and service evaluators will have the chance to control the lifecycle of their SafeCity Phase 2 applications in an integral, end-to-end fashion.

SEs

Phase 1

Interface Layer SE, Data Manager Layer SE, Service Layer SE

Extension of these semantic SEs from Phase 1 in order to provide a unified semantic description of the holistic platform. This

is necessary so that the higher-level tools described in the SEs below provide stakeholders with an easier-to-understand model of the inner working of the SafeCity Phase 2 platform.

Phase 2

SafeCity2 Platform Manager SE

This SE will be in charge of managing the distribution and operation of the third party services created. A marketplace of services will be provided to end users, who will be able to browse, review and purchase services for their usage. Different end-user profiles will be implemented: technologist, systems integrator, end-user (e.g., city council).

Workflow Manager SE

The building of any application based on the SafeCity2 API involves a number of elements and flows of information. This SE will provide the means to give end users a tool to easily model their SafeCity2 case studies and their data inputs and outputs. This will be later used for simulations or storage and offline analysis.

FIWARE GEs:

Cloud Object Storage GE

Metadata Preprocessing GE

Apps USDL GE, Apps Repository GE and Apps Registry GE

Apps Marketplace GE

Apps RSS GE

Apps Mediator GE

Apps Composition Editor GE, Apps Composition Execution GE

Furthermore, the *Cloud.PaaS GE*, *Developer Tools.API IDE support GE* and *Developer Tools. FI-CoDE Basic Framework GE* will be deployed

4.2.10 APP10 - Performance Monitoring and Evaluation Tools

APP10 - Performance Monitoring and Evaluation Tools
SCOPE – SHORT DESCRIPTION OF FEATURES/CAPABILITIES
The goal of this application is to provide performance monitoring and evaluation tools for SafeCity Phase 2 trials in order to objectively evaluate the performance of APPs in the context of the implemented public safety case study solutions. For this purpose, data logging from each APP (SEs and GEs) for the defined performance criteria (response times, quality of service, false alarm rates, etc.) will be collected and subsequently analyzed using data mining and statistical analysis tools to infer and visualize the collective performance and most importantly, spot cases of faulty operation and thus provide feedback back to APPs to properly tackle and overcome such cases. Reports will be generated based on the analysis of the results and will permit the elaboration of conclusions and lessons learned per trial site.
SEs
Phase 1
None
Phase 2
Performance Visualization Tool SE - provides the GUI interface of performance counters and performance analysis results; it features multiple graph views that enables the user to visually review the analyzed performance log data
Data Collection Manager SE – enables the customization of the type of performance data to be collected and stored in logs; defines interfaces for adding data from external/offline sources; it can be associated with rules of scheduling for data collection at specific times.
Performance Data Analysis SE – provides the means to analyze collected log/performance data per defined performance criterion and functional operation and discover automatically patterns showcasing normal operation and performance as well as cases of irregular performance due e.g. to faulty operation or low performance in specific deployed contexts.

Forwards the results for visualization and to be assessed for feedback to the APPs. It incorporates a rich set of data mining and machine learning algorithms for data analysis and pattern discovery.

Performance Assessment SE – it derives the results of performance data analysis and within specific contexts of deployment, based on predefined rules (e.g. thresholds for normal or faulty operation) assesses such situations in order to generate automated alerts and respective actions forwarded to the Reporting Manager SE. There may cases that such situations are manually triggered by operators after visualizing the results of data analysis.

Reporting Manager SE – responsible for generating of reports, and viewing of past performance data in a variety of ways. ; define thresholds for alerts and automatic actions

FIWARE GEs

Tools.Application Testing Support Tools

Cloud.Monitoring GE

Cloud.MonitoringAnalytics GE

5. Characterization of potential infrastructures

5.1 Characterization of potential infrastructures according to SafeCity Global Framework

This section aims to define and characterize the cities' potential infrastructures that could be interesting for SafeCity Phase 2 taking into account the Global SafeCity Framework Characterization defined in the deliverable D3.2 and the Cities Framework Characterizations defined in the deliverables D3.3 (Madrid), D3.4 (Bucharest) and D3.5 (Stockholm).

For this characterization, it has been taken as input the Guidelines for Infrastructure Evaluation Metrics given in D3.3, D3.4 and D3.5, and the Guidelines for Cities SafeCity Framework Characterization and scoring provided in D3.2, and it has been analyzed which are the metrics applicable for each of the Future case studies and tried to characterize the minimum needed infrastructures in terms of applicable metrics.

5.1.1 Potential infrastructures according to Madrid Framework Characterization

This sub-section describes the potential infrastructures in the city of Madrid that could be part of the Phase 2.

According to the deliverable D3.3, the envisaged five future case studies can be classified in three main groups:

1. Citizens Behavior
    a. Enhanced detection and tracking of a suspicious citizen
    b. Early detection of a suspicious abandoned backpack and evacuation order in a public space
2. Traffic Incidents Management
    a. Early detection and response for critical changes in road condition
    b. Early detection and warning of an environmental incident (fire, flood …)
3. Ad-hoc networks
    a. Intelligent and trustworthy management of large events

Below, it is given the minimum characteristics that the infrastructures should comply in order to be able to be used in each of the future Case Studies.

Comparison criteria	Description	Comparison metrics (objective/subjective)	Applicability to the case studies
Existing CCTV network in the city.	Madrid city manages over 3.000 video cameras along all the city, most of them are traffic cameras or public building protection ones. There are also cameras in vehicles, Service Tunnels and video surveillance cameras in streets. All the video surveillance cameras locations in streets are available to SafeCity, as is the MCC network and other elements as power, arms, etc. For the Case Study will be used "new" cameras in the same locations of the current ones, and using the MCC ICT infrastructure. Subjective narrative evaluation of the existing CCTV network in the city focusing on the elements not described in the objective scoring such as access rights to the camera network and terms of usage.	Objective data of the network: • Number of elements accessible to SafeCity : ○ Over 120 camera locations ○ MCC IP street network: FO up to 4Gbps ○ MCC IP network from CCTV to C2 centers: FO up to 10Gbps • Image quality aspects of the current cameras: ○ Codec : mpeg4 and jpg ○ Resolution: VGA (640 x 480) ○ Frames per second: up to 30 ips ○ Chroma subsampling: Color (30 IRE): 0.7 lux ○ Bandwidth per stream max 4,096 kbps Subjective 0-5, with: • 4	(1a), (1b), (2a), (2b), (3) NOTES: • For (1a), (1b): 5 CCTV • For (2a), (2b): 10 CCTV • For (3): 15 CCTV • Medium/high image quality aspects • There is a network of cameras but there are difficulties (e.g., network too small, terms of usage of images not optimal)
Internet connectivity available in the City.	Evaluation of the internet connectivity available in the City.	Objective data and figures on the following: • Wired connectivity options: ADSL 10Mbps/820 kbps: 25€/month VDSL 30Mbps/ 1Mbps: 30€/month FTTH 100Mbps/ 10Mbps: 40€/month FTTH 100Mbps/100Mbps: 100€/month • Wireless connectivity options: HSDPA 7,2 Mbps/5,7 Mbps: 40 €/month Subjective 0-5 with: • 4	(1a), (1b), (2a), (2b), (3) NOTES: • For (1a), (1b), (2a),(2b): Good wired connectivity required • For (3): Good wired and wireless connectivity required • There are available options that fulfil the needs for SC but they are not completely optimal: one of wired or wireless is not good enough, prices are very high for the required bandwidth or the bandwidth is very tight for our requirements.

Alerting capabilities available in the City	Evaluation of the alerting capabilities available in the City	Objective data and figures on the following: • Number of information displays throughout the city: traffic, environmental and others • Typical response times to changes in these displays - Number of Traffic variable information displays: 170 - Number of variable information displays of the City Public Transport: 362 response time= 0 (automatic update) • Other means accessible to alert citizens: traditional media, targeted SMS systems Via FM/AM radio broadcasting Subjective appraisal by SC consortium • 4	(2a), (2b), (3) NOTES: • For (2a): 2 information displays throughout the city , 5 minutes for changes in these displays and panels in roads • For (2b): 5 information displays throughout the city , 1 minutes for changes in these displays and panels in roads • For (3): 5 information displays throughout the city , 0,5 minutes for changes in these displays, and target SMS systems and interactive panels • There are at least some available alerting systems (panels, etc.) that may be used by SC.
Existing Road Sensor Networks for the City	Appraisal of the existing Road Sensor Networks for the City	Objective data and figures on the following: • Number of network elements • Sensing capabilities for the network: road condition, traffic flow. - 7000 road sensors - response time= 0 (automatic send & update)	(2a), (2b), (3) NOTES: • For (2a), (2b): 10 road sensors in the network, high sensing capabilities The City has a very complete network of sensors that is fully

		Subjective SC scoring (0-5): • 4	usable by SC and doesn't require significant improvements. • For (3): 7 road sensors in the network, high sensing capabilities • There are existing road sensor networks which provide data on at least several of the target metrics of interest by SC and they are at least possible to access by our applications. Authorities co-operate in the joint installation of extra equipment.
Environmental Sensor Networks	Appraisal of the existing Environmental Sensor Networks for the City	Objective data and figures on the following: • Number of network elements • Sensing capabilities for the network: e.g., weather, pollution, seismic activity. - 25 stations around the city for air quality - 30 stations for acoustic level - 3 main weather stations - capabilities: PM10; PM2.5; SO2; CO; O3; NO2; BEN; TOL; noise; weather Subjective SC scoring (0-5): • 4	(2a), (2b), (3) NOTES: • For (2a), (3): Medium capabilities mainly for weather and pollution. There are existing environmental sensor networks which provide data on at least several of the target metrics of interest by SC and they are at least possible to access by our applications. Extra equipment may be installed by SC. • For (2b): Good capabilities for all kinds. The city has a very complete network of environmental sensors that is fully usable by SC and doesn't require additional effort in new equipment.

Command Centres	Evaluation by the application leaders of the C2 capabilities of the City	Objective data and figures on the following: • Number of C2 centres in the city - city council C3 center : CISEM - national police C2 center: 091 • Coverage of the required area by the Case Study. - 100 % • Connectivity to sensing infrastructure: e.g., traffic data, CCTV network - Fiber optic, satellite, WIMAX, 3,5G, ADSL • Connectivity to PS bodies, first responders: police, fire fighters - TETRA radio - 3,5G • Number, qualification of staff in the facilities **CISEM city council employees** - 200 police officers - 40 fire fighters - 50 Emergency medical personnel - 18 Traffic agents - 10 technicians	(1a), (1b), (2a), (2b), (3) NOTES: • For (1a), (1b): 1 C2 centre in the city, good connectivity to CCTV, connectivity to police • For (2a), (2b), (3): 1 C2 centre in the city, good connectivity to traffic data and CCTV connectivity to police and fire fighters • At least one Command Centre is accessible for SC purposes and that the facilities are at least partly usable by our applications. The staff is at least competent enough to go through a SC training course.
		Subjective SC scoring (0 to 5): • 4	

Table 2 Recommended potential infrastructures' metrics according to Madrid Framework Characterization

5.1.2 Potential infrastructures according to Stockholm Framework Characterization

This sub-section describes the potential infrastructures in the city of Stockholm that could be part of the Phase 2.

According to the deliverable D3.5, three of the five case studies described in D3.2 are applicable in the city of Stockholm[3]:

a. Early detection and response for critical changes in road condition

b. Early detection and warning of an environmental incident(fire, flood)

[3] The case studies 2enhanced detection and tracking of a suspicious person" and "early detection of a suspicious abandoned backpack and evacuation order in a public space" are not applicable in the Stockholm region as there are no CCTV networks at the street level.

c. Intelligent and trustworthy management of large events

Below, it is given the minimum characteristics that the infrastructures should comply in order to be able to be used in each of the future Case Studies.

Comparison criteria	Description	Comparison metrics (objective/subjective)	Applicability to the case studies
Existing CCTV network in the city.	There are currently no CCTV networks used in the Stockholm region at the street level. There is a CCTV network installed in the public transport system, including all subway stations, buses, in most subway cars and in the latest deliveries of commuter trains. The public transport system is however considered as a private area. The CCTV network is operated from the Stockholm Transport Safety Centre.	Objective data of the network: • Number of elements accessible to SafeCity: *None* • Image quality aspects: *Not applicable* Subjective 0-5, with: • *0 (no CCTV network at the street level)*	Not applicable
Internet connectivity available in the City.	Wired connectivity options in the Stockholm region consist of: • DSL-connection (telephone socket) • City WAN (TV-socket, LAN-socket) • Fiber optic WAN (LAN-socket) Wireless connectivity options consists of: • Three GSM/GRPS-networks • Two 3G-networks (HSDPA/HSUPA) • Two 4G-networks (LTE) • One CDMA 2000-network (Rev B) • Several hundred Wi-Fi hotspots (IEEE 802.11)	Objective data and figures on the following: • Wired connectivity options: *(a) DSL*, <60 mbsp/<20 mbps, no limit in GB, 47.3 €/month incl. VAT. *(b) City WAN*, <1000 mbps/<100 mbps, no limit in GB, 94.7 €/month incl. VAT. *(c) Fiber optic WAN*, <1000 mbps/<1000 mbps, no limit in GB, incl. priority in the network, 415.1 €/month excl. VAT. • Wireless connectivity options: *(a) 3G*, 20-30 mbps/<5.6 mbps, incl. 30 GB and access to Wi-Fi hotspots, 31.9 €/month excl. VAT. *(b) 4G/3G*, <100 mbps/<50 mbps, incl. 30 GB and access to Wi-Fi hotspots, 47.3 €/month excl. VAT. *(c) CDMA 2000*, <9.3 mbps/< 5.4 mbps, incl. free roaming in Scandinavian countries, 35.5 €/month incl. VAT. Subjective 0-5 with: • *5*	(a), (b), (c)

Alerting capabilities available in the City	There two main groups of alerting capabilities – for public alerts and warnings and for traffic warnings. General alerting capabilities consist of a variety of alerting systems (see below) that are connected to the nationwide public warning system recognized as the so called VMA-system. The VMA-system includes the following alerting systems: • Sirens • TV and radio/RDS • Web and social media • Mobile PA-systems • CB • SMS (subscription) Traffic warning capabilities – similar to the general alerting capabilities – consist of a variety of alerting systems (see below) that are connected to the nationwide traffic management system recognized as NTS. The following systems are included in NTS: • TV and radio/RDS • Web • PA-systems in the public transport system • DRIP-signs • RDS-TMC • Voice messaging services	Objective data and figures on the following: • Number of information displays throughout the city: *Not available* • Typical response times to changes in these displays: *Real-time* • Other means accessible to alert citizens: *(a) General alerts and warnings: TV and radio/RDS, sirens, CB, web pages and social media, and SMS.* *(b) Traffic warnings: TV and radio, web, social media, DRIP-signs, RDS-TMC, PA-systems in the public transport system, voice messaging services.* Subjective appraisal by SC consortium • *4 (accessibility for SafeCity unknown)*	(a), (b), (c)
Existing Road Sensor Networks for the City	There is a nationwide traffic management system recognized as NTS, to which different local, regional and national road sensor networks are connected. The sensor networks consist of weather, optical, IR and other types of sensors.	Objective data and figures on the following: • Number of network elements: *800+ sensor stations (figure for the entire country).* • Sensing capabilities for the network: *Weather, road surface condition and traffic flow.* Subjective SC scoring (0-5): • *5 (accessibility for SafeCity unknown)*	(a), (b)

Environmental Sensor Networks	There is a citywide sensor network, which is connected with other local sensor networks into a region wide network. The sensor networks are connected to a web based system Airviro, which integrates diverse modules, such as for data collection, simulation and dispersion modelling, and web publishing. ad sensor networks are connected. The sensor networks consist of weather, optical, IR and other types of sensors.	Objective data and figures on the following: • Number of network elements: *In the City of Stockholm there are 8 fixed sensor stations. The total number of sensor stations in the Stockholm region is 15. Mobile sensor stations are also used; their number is unknown.* • Sensing capabilities for the network: *Air quality/pollution (15+ different substance classes) and weather.* Subjective SC scoring (0-5): • *5 (accessibility for SafeCity unknown)*	(a), (b)
Command Centres	There is a number of different command and control centres in the Stockholm region.	Objective data and figures on the following: • Number of C2 centres in the city: *(a) Public safety (operational services) – 5 fixed and 5+ mobile C2 centres, (b) Transportation – 5.* • Coverage of the required area by the Case Study (case study in Phase 1): *3 C2 centres (2 fixed and 1 mobile).* • Connectivity to sensing infrastructure: *NTS (traffic related information), 112-and incident management platform (emergency call, resources) combined with TETRA and AVL.* • Connectivity to PS bodies, first responders: *Data (fiber, ADSL, wireless), telephony (wired, IP, TETRA.* • Number, qualification of staff in the facilities: *Not available* Subjective SC scoring (0 to 5): • *5 (relates to C2-centres involved in the Phase 1 case study; for other C2-centers accessibility for SafeCity unknown);*	(a), (b), (c)

Table 3 Recommended potential infrastructures' metrics according to Stockholm Framework Characterization.

5.1.3 Potential infrastructures according to Bucharest Framework Characterization

This sub-section describes the potential infrastructures in the city of Bucharest that could be part of the Phase 2.

According to the deliverable D3.4, the five future case studies taken into account can be classified in three main groups:

1. Citizens Behavior
    a. Enhanced detection and tracking of a suspicious citizen
    b. Early detection of a suspicious abandoned backpack and evacuation order in a public space
2. Traffic Incidents Management
    a. Early detection and response for critical changes in road condition
    b. Early detection and warning of an environmental incident (fire, flood …)
3. Ad-hoc networks
    a. Intelligent and trustworthy management of large events

Comparison criteria	Description	Comparison metrics (objective/subjective)	Applicability to the case studies

Existing CCTV network in the city.	There is a CCTV network installed in district 2, the most secure area of Bucharest.
	There are 480 cameras installed in all the neighborhoods of district 2 and by the end of the project the district will be monitored by 719 surveillance cameras.
		Objective data of the network:
		• Number of elements accessible to SafeCity
		• Image quality aspects:
		  ○ Codec
		  ○ Resolution
		  ○ Frames per second
		  ○ Chroma sub-sampling
		  ○ Bandwidth per stream
			(1a),(1b)

		Subjective 0-5, with: • *5*	
Internet connectivity available in the City.	Wired connectivity options in the Bucharest region consist of: • DSL-connection (telephone socket) • City WAN (TV-socket, LAN-socket) • Fiber optic WAN (LAN-socket) Wireless connectivity options consists of: • Three GSM/GRPS-networks • Four 3G-networks (HSDPA/HSUPA) • Two 4G-networks (LTE) Several hundred Wi-Fi hotspots (IEEE 802.11)	Objective data and figures on the following: • Wired connectivity options, bandwidth and pricing in euro for the City (e.g. DSL 3mbps/1mbps: 40€/month, FTTH 50mbps symmetric: 100€/month) • Wireless connectivity options: bandwidth, bandwidth cap and pricing in euro for the city (e.g., 3G 7.2 mbps/3.6 mbps 1GB/month 45€/month)	(1a),(1b),(2a)
		Subjective 0-5 with: • *5*	

Alerting capabilities available in the City	Evaluation of the alerting capabilities available in the City	Objective data and figures on the following: • Number of information displays throughout the city: traffic, environmental and others • Typical response times to changes in these displays • Other means accessible to alert citizens: traditional media, targeted SMS systems	(1a),(1b)
		Subjective appraisal by SC consortium • *3*	
Existing Road Sensor Networks for the City	Appraisal of the existing Road Sensor Networks for the City	Objective data and figures on the following: • Number of network elements • Sensing capabilities for the network: road condition, traffic flow.	Not applicable
		Subjective SC scoring (0-5): • *0*	
Environmental Sensor Networks	Appraisal of the existing Environmental Sensor Networks for the City	Objective data and figures on the following: • Number of network elements • Sensing capabilities for the network: e.g., weather, pollution, seismic activity.	Not applicable
		Subjective SC scoring (0-5): • *0*	
Command Centres	There is a number of different command and control centres in the Bucharest region.	Objective data and figures on the following: • Number of C2 centres in the city • Coverage of the required area by the Case Study. • Connectivity to sensing infrastructure: e.g., traffic data, CCTV network • Connectivity to PS bodies, first responders: police, fire fighters • Number, qualification of staff in the facilities	(1a),(1b),(2a)
		Subjective SC scoring (0 to 5): • *5*	

Table 4 Recommended potential infrastructures' metrics according to Stockholm Framework Characterization.

5.2 Characterization of INFINITY potential infrastructures

This section aims to define/characterize the potential infrastructures identified from XiPi Repository that could be interesting for SafeCity Phase 2, taking into account the Global SafeCity Framework Characterization defined in the deliverable D3.2.

Below, you can find the potential infrastructures identified through XiPi Repository and that could be identified interesting for SafeCity Phase 2 project.

Barcelona Smart Cities Pilot Network at 22@ District and WIFI/WIMAX Network (30% of the Urban City area: 469 Nodes) (Spain)

This Infrastructure could be used in the following Case Studies:

- Enhanced detection and tracking of a suspicious person
- Early detection of a suspicious abandoned backpack and evacuation order in a public space

They have a Wireless Sensor Pilot Network for sensoring and Smart Cities applications, located at 22@ district with five different platforms and 200 sensors.

They use 802.15.4, Zigbee, 802.15.1 and 802.11, and therefore, they could be used for SafeCity2 applications.

6net / Kuuskaista (Finland)

This infrastructure can be used as a backbone for the following municipalities in Finland: Kuortane, Alavus, Töysä, Ähtäri, Lehtimäki village of Alajärvi, Soini.

This infrastructure could be used in the following Case Studies:

- Detection and tracking of a suspicious citizen

Acreo National Testbed (Sweden)

The Acreo National test-bed is a live network for Internet, IPTV and telemetry services, with a small number of end users, connected via FTTH, LTE or OTT. Here, services may be evaluated by end users, prototypes may be integrated into the test network, demonstrations may be performed, and interoperability tests may be performed.

Also, the traffic monitoring framework, in which Acreo collects IP traffic data from partners (municipal networks) is a part of the test-bed, and will provide input to the knowledge base on user behaviour, traffic patterns and QoS, QoE analysis.

This infrastructure could be used in the following Case Studies:

- Detection of critical environmental changes in road condition
- Early detection and response for critical changes in road condition
- Detection and tracking of a suspicious citizen

Bonfire (ES)

BonFIRE offers an experimenter control of compute, storage and networking resources. BonFIRE supports dynamically creating, updating, reading and deleting resources throughout the lifetime of an experiment. Compute resources can be configured with application-specific contextualisation information that can provide important configuration information to the virtual machine; this information is available to software applications after the machine is started.

BonFIRE also supports elasticity within an experiment, i.e., dynamically create, update and destroy resources from a running node of the experiment, including. cross-test-bed elasticity.

This infrastructure could be used in the following Case Studies:

- Detection and tracking of a suspicious citizen

CISEM (Spain)

It is an advanced emergency command & control center, which integrates information, systems, and people for managing emergencies and security of the City of Madrid. CISEM (coordinates the various services involved with disaster or major event risk for incidents of emergency management in critical infrastructure in the city of Madrid, offering security and unified treatment of emergencies. CISEM was launched on January 16, 2007.

This infrastructure could be used in the Phase 2 Case Studies, as the command and control center, and also as it was used in SafeCity Madrid PoC.

CONSORZIO NAZIONALE INTERUNIVERSITARIO PER LE TELECOMUNICAZIONI (CNIT) (Italy)

CNIT operates 3 National Laboratories, 3 Local Laboratories and a national broadband satellite network

This infrastructure could be used in:

- Early detection and warning of an environmental incident

e-lab (Norway)

They have build about 800 - 1000km fiber optic network in the region Troms County.

Today, the infrastructure is based on PTP usage but e-lab is only based on dark fiber in our core fiber optic network. The e-lab infrastructure will extend over the whole region.

This infrastructure could be used as a backbone for SafeCity 2 applications

Emersat (Italy)

Emersat project aimed to realize a pilot network and a pilot service tailored on Civil Protection needs, based on satellite infrastructure.

This infrastructure could be used in:

- Early detection and warning of an environmental incident

European Traffic Observatory Measurement Infrastructure (Hungary)

ETOMIC is a measurement infrastructure in Europe that is able to carry out high temporal resolution (~10 nano second), globally synchronized, active measurements between measurement boxes. It provides a high resolution, spatially extended dynamic picture of fast changes in the network traffic. This can open up the possibility to new kind of network tomography, where cross correlation between measurement flows can be measured on a fine timescale and the internal state of the network, far away from the ends of the network, where the measurement devices are located, can be reconstructed, its time behavior can be studied, and the data can be analyzed with methods developed in the complexity science literature.

This infrastructure could be used in the following Case Studies:

- Detection of critical environmental changes in road condition
- Early detection and response for critical changes in road condition

FOKUS Smart Communications Playground (Germany)

The Smart Communications Playground is a pioneering reference test-bed focusing on the provisioning of (tele-)communications service capabilities for human-to-human and machine-to-machine (M2M)

services based on state-of-the-art Service-Oriented Architecture (SOA) principles. The main focus is on the provisioning of a generic service platform, communication and connectivity interfaces for various service verticals.

This vendor- and provider-independent technology playground is an open test-bed for service platforms on top of converging fixed and mobile broadband networks, IMS and Machine-Type Communication networks. The main focus lies in the research and development of new technologies, designs, and ideas for:

- Distributed service orchestration and composition with real-time constraints
- Service brokerage for OTT & telco services
- Network abstraction and M2M APIs
- Open client infrastructures
- Virtualization of service infrastructures

This infrastructure could be used in the following Case Studies:

- Detection and tracking of a suspicious citizen
- Early detection of a suspicious abandoned backpack
- Detection of a not allowed entry into a secure area

FOTSIS (Spain)

FOTsis is a large-scale field testing of the road infrastructure management systems needed for the operation of seven close-to-market cooperative I2V, V2I & I2I technologies (the FOTsis Services), in order to assess in detail both 1) their effectiveness and 2) their potential for a full-scale deployment in European roads.

Specifically, FOtsis will test the road infrastructure's capability to incorporate the LATEST cooperative systems technology at 9 Test-Sites in four European Test-Communities (Spain, Portugal, Germany and Greece), providing the following services:

- S1: Emergency Management
- S2: Safety Incident Management
- S3: Intelligent Congestion Control
- S4: Dynamic Route Planning
- S5: Special Vehicle Tracking
- S6: Advanced Enforcement
- S7: Infrastructure Safety Assessment

Using an integral and comprehensive approach, FOTsis will therefore review the road infrastructure and communication networks required to secure a proper connectivity from the traffic control centers (and all the information they already have available, enhanced with the V2I data) with the users/vehicles.

Relying on the common European and open ITS architecture guideline proposal (supported by the project COMeSafety), able to incorporate available and future ITS services and systems, FOTsis aims to contribute to the safety, mobility and sustainability challenges faced nowadays by the European road

transport system. The project represents a major step forward to better connect vehicles, infrastructures and traffic management centers, the main focus being placed on the responsibilities of the road operator.

This infrastructure could be used in the following applications:

- Detection of critical environmental changes in road condition
- Early detection and response for critical changes in road condition

Trondheim Pilot (Norway)

As Trondheim Pilot has ambitious environmental targets (20% reduction in emissions by 2018), the main focus is “green” services, including multimodal applications. It will be possible to exploit the availability of a wide range of existing data and infrastructure, including:

- 25 fibre-connected roadside units for 5.9 GHz communication (using IEEE 802.11p), plus vehicles equipped for V2I and I2V data exchange. The RSUs cover over 6 km of streets in city centre area.
- A total of approx 330 FEVs (including the municipal fleet) and 73 electric charging stations.
- A speed monitoring system (using AutoPASS tags already installed on approx 85% of vehicles in Trondheim) with 25 measurement stations, covering 21 roads within the arterial network.
- Real time bus ETA information (currently communicated via panels at c 100 bus stops plus mobile phones). Also bus arrival warning service for visually impaired passengers.
- Traffic flow and signal phase data for 70 intersections (equipped with traffic-adaptive signaling with priority for selected PT vehicles) and connected with RSUs.

This infrastructure could be used in the following Case Studies:

- Early detection and response for critical changes in road condition

6. Test-bed pre-selection

This section aims to analyze the test-beds pre-selected for Phase 2 starting from the information collected in the Section 3 - Plan for User Community Building and the Section 5 - Characterization of Potential Infrastructure, in addition to the information that has been provided directly by the cities.

For each test-bed, it is considered the following information:

- Test site and motivation
- Potential infrastructures to be used
- Communities involved
- Ethical and Legal Framework

6.1 Madrid Test-bed

6.1.1 Test site and motivation

The test site in the city of Madrid will be AZCA (which stands for Mixed Association for Compensation of the A Block of the Commercial Area of the Avenue of Paseo de la Castellana), one of the main financial districts of Madrid. This complex is composed of towers that are between 80 and 160 meters high, department stores, shopping malls, restaurants and a large pedestrian area that's above car parks, tunnels and underground pedestrian galleries.

Figure 5 Google Earth image of AZCA

This area is also known for its nightlife. Bars, pubs, restaurants and discotheques can be found under the arches or on the ground floor of the buildings. These zones become home of disturbances and gang violence that have caused a reputation of problematic and most troubled area of Madrid, especially during weekend nights. Residents and stores keep on claiming for more protection due to remarkable disturbances and riots.

Hence, this area has two sides, mixing the business and commercial side during daylight and agitated leisure time at nights.

Consequently, the basic line of action of Madrid City Police is to install video surveillance systems in sensible areas of the city where there is a clear demand of the society. Hence, it would fit with AZCA needs, answering the security related problems in the zone as the citizens and businessman requests.

6.1.2 Potential infrastructures to be used

Nowadays, Madrid City Council counts on the AZCA Monitoring and Control Center, named Lightening and Access Galleries Control Centre of Madrid Municipality. In order to make efficient use of resources and reusing as most existing infrastructure as possible, these centre facilities will be presented as the best place to instantiate the local center tasks required for SafeCity solution in Phase 2. This center already counts on broadband connectivity to the communication network of Madrid municipality so there is no need to install any SDH/PDH communication node to this fiber optic ring network.

Also, Madrid City Council relays on different centers to manage the information coming from the surveillance system currently deployed. The main center is CISEVI (Integrated Video Signal Center), which manages the video surveillance system, providing the images under request to the other centers as CISEM (Integrated Centre of Emergencies in Madrid). Both centers are connected to the municipality network and available for Phase 2 as part of the existing infrastructure to be used during the test.

Finally, it is noted that different telecommunication operators offer broadband connection in the area (xDSL, fiber Optic). Besides, mobile 3G devices will be also used to provide surveillance information to the system. Subscribed citizens' devices, deployed policemen or patrol vehicles may enter on-site information through public mobile networks.

6.1.3 Communities involved

Both authorities and AZCA residents/commercials claim for a secured area and therefore, they will participate easily in the trials. During Phase 2, SafeCity will count on the real involvement of Madrid City Council, who will lead the trials performance in this test site. In addition, several residents and commercial associations, who have actively requested higher security measures to the City Hall in AZCA surroundings, have been identified as potential real users of the system. These are:

- *COMUNAZCA,* which is the Association of neighborhood-community presidents of Orense/Azca St.
- AZCA Businessman and Traders Association.
- La Viña Association, which is the Community of Madrid Hotel Business Association.

6.1.4 Ethical and Legal Framework

SafeCity has already performed a detail analysis of the ethical and legal aspects of deployment of a video-surveillance system in Madrid. In summary, relevant Spanish regulations are the Personal information Protection Law 15/99 and the Right to Honor Civil Protection, personal and family privacy and image Law 1/1982.

There is a number of requirements established with the purpose of guaranteeing the fundamental rights of people eventually recorded. Handling of sensitive data (e.g. personal data as criminal records, license plates, recorded images) should cope with certain constraints. For instance, sensitive data must be physically protected, and securely encrypted for transmission over public networks. CCTV cameras should have a dynamic masking technology in the way that private spaces are not recorded. The maximum storage time of recorded watermark images in Spain as in most of the EU member states is 7 days.

Also, there are specific procedures that regulate the installation and use of the video surveillance systems in public places in Madrid. This installation will have to be authorized by the Madrid Commission of Surveillance Guarantee and each of them will have to pass the test of proportionality

which is essential to determine the legality of any restriction on fundamental rights. In addition, the approval of Security Area of Madrid City Council is required.

Regarding bulk SMS delivery to Citizens mobile devices, it is allowed by Spanish regulation only under subscription and consent of citizens.

Regarding user-generated content, the citizens willing to report real-time information related to potential unsafe situations will have to subscribe to the service authorizing the usage of their content by the authorities.

6.2 Athens Test-bed

6.2.1 Test site and motivation

Athens holds the top place in the set of EU countries for traffic deaths: 8.200 accidents occur in average every year caused mainly by the road traffic density.

The Athens Traffic Management Centre (ATMC) operates under the auspices of the Attica Region Administration and is responsible for regulating road traffic in the wider area of Athens. According to ATMC statistics, car accidents represent approximately 30% of the cases creating road traffic problems.

There are two challenges for mitigating the impact of such situation. On one hand, ATMC is interested in the early detection of car accidents in locations where traffic is denser and so, ATMC has selected a number of micro-sites in the city of Athens based on car accident statistics in which the early crash detection and notification services could be required: *Patision* with *Solomou* Street, *Syggrou* Avenue with *Petmeza* Street, *Kifissias* Avenue with *Panormou* Street and *Pireos* Avenue with *Persefonis* Street.

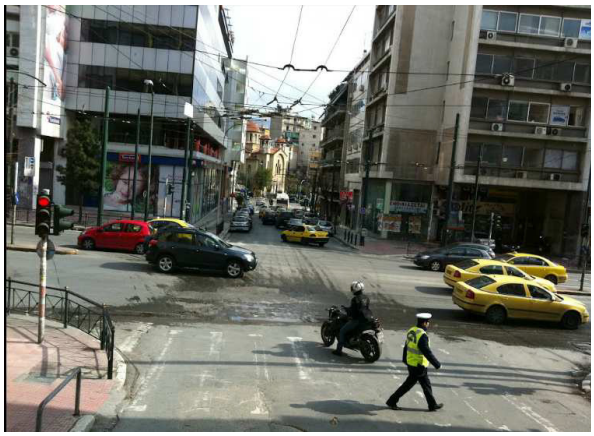


Figure 6 Crossroad in Patision with Solomou Street

On the other hand, ATMC is also demanding smart tools to identify the best regulation of traffic flow that reduces the probability of car accidents based on traffic video surveillance. For this necessity, ATMC has defined the Leoforos Marathonos (Marathonos Avenue), concretely, in the intersections Pikermi, Rafina and Nea Makri.

6.2.2 Potential infrastructures to be used

The traffic surveillance cameras in crossroads to be used for the tests were already installed in the metropolitan area of Athens by authorities. There are 208 traffic cameras and they are operated on a permanent basis by the Athens Traffic Management Centre (ATMC).

The whole surveillance system installed includes the local video recording enabling operators to retrieve video and pictures. This system uses wired fiber optics infrastructure and large databases of information arranging events according to the following typology: accidents, marches, public works, damaged cars, weather and extraordinary events. In addition, raw data are publicly available on a charge basis.

During Phase 2, ATMC will provide to SafeCity with real time data from a number of road cameras for testing purposes. In addition, it is contemplated the deployment of additional cameras at some places which will also count of the fiber optic communication network and local operation centers facilities to installed electronic hardware.

6.2.3 Communities involved

The close participation of the Athens Management Control Centre (ATMC) and the participation of KEMEA will guarantee the involvement of the authorities.

6.2.4 Ethical and Legal Framework

SafeCity has already performed a detail analysis of the ethical and legal aspects of deployment of a video-surveillance system in Athens. There is an extended and strict legislative framework regarding the use of surveillance systems in public areas in Greece as the Article 8 of the European Treaty on Human Rights for the protection of private life, Convention 108/1981 of the Council of Europe for the protection of Individuals with regard to Automatic Processing of Personal Data (validated by the Greek Law L. 2068/1992), Directive 95/46/EC of 24 October 1995 for the protection of natural persons with regard to the processing of personal data and also for the free circulation of these data, L. 2472/97 on the protection of individuals with regard to the processing of personal data and L. 3917/2011 which excludes Hellenic Police from the application of the L.2472/97.

In summary, it can be outlined that in Greece there are clear restrictions regarding the use and operation of the CCTV systems in public places for security purposes. However, there is a less restrictive new law on-going which allows a more extended use of data and information from CCTV networks.

6.3 Turin Test-bed

6.3.1 Test site and motivation

Turin is the capital of the Piedmont region and one of the major business and cultural centre in northern Italy. The test site in the city of Turin will be in *Barriera di Milano*, a well-defined 2 km^2 area in the suburbs area of Turin characterized by a concentration of economic and social problems, and perceived by citizens as a dangerous area. The park near *Mercadante* Street, the open air market in *Foroni* Square and the main streets in this zone are the key areas of interest to the authorities to have the Safety and Security capabilities of the SafeCity system.

Figure 7 Key areas of interest: the park near *Mercadante* Street (left), the open air market in *Foroni* Square (centre) and the main streets in *Barriera di Milano* zone (right).

Indeed, Turin City Council is conducting a *Torino Smart City Project into Barriera di Milano* zone which aims at deploying Smart City infrastructures. The *Barriera di Milano* Urban Plan covers a period of short-term, but it gets in a scenario of large urban transformations to be realized from medium to long period. Turin City Council (TCC) aims at increasing in a smart way the surveillance systems in the three proximate areas in order to end with the anti-social behavior of certain pedestrians, i.e. the vandalism against the public bicycle sharing facilities and other public furniture, the drug-related crime, breaking into cars, robbery and burglary and other alcohol-related crime.

6.3.2 Potential infrastructures to be used

The test relies on the smart public light grid that counts on broadband connectivity through power lines (PLC) and mobile (LTE) connections, and whose public lampposts capillarity can be used as hot spots for the *Connected City,* behaving as a new surveillance information source for operators.

Turin City Council provides several existing infrastructures to be used within the test site as considered: the existing public lighting system, cameras with local storage and their control infrastructure and Police station premises in the area. In addition, Telecom Italia, who will be the Turin Test-bed Technical Director, will be in charge of the additional equipment installation, the provision of broadband Internet access (being PLC and 3G/4G or LTE) and preparation of the entire required infrastructure.

On the other hand, Turin City Council is pioneer in providing Open Data city portal offering public categorized information (e.g. list of proximate road-works in Turin city, list of headquarters of police, list of hospitals and pharmacies in Turin city), that is an important source of information to aggregate to the surveillance information and inform the safety-services subscribers.

6.3.3 Communities involved

During Phase 2, SafeCity will count on the real involvement of Turin City Council and willing to participate offering existing equipment and facilities in the area as trials experimentation sites. In addition, the SafeCity Consortium has established contact with UPTU7, that is an Internet Forum for Citizens, Public Administrations and Associations specifically dedicated to the city security in which Turin City is actively involved.

6.3.4 Ethical and Legal Framework

Italian Citizens Privacy Law established certain relevant ethical implications related to video and audio surveillance systems. Indeed, the Investigative Unit of the Metropolitan Police of Turin has a large expertise on these surveillance implications.

Regarding the Italian relevant laws applicable to video surveillance regulations appear the C*odice della Privacy* law about the town surveillance. It specifies certain security measures regarding the preservation of the movie files that cannot be kept for more than seven days or the people must be alerted with a special sign that the area is subject in video surveillance. However, The *Codice della Privacy* is not applicable in the field of video surveillance on public ground where Judicial Police investigations are in progress, since it must respect the Italian Code of Criminal Procedure in this case.

6.4 Bucharest Test-bed

6.4.1 Test site and motivation

The test site in the city of Bucharest will be the *Obor Market* (*PiaŃa Obor*). The *Obor Market* has been the Bucharest's largest public market for many years and has suffered numerous changes and irregular expansions. It is located in the Bucharest Sector 2 district, a north-east district of Bucharest.

Today, the *Obor Market* counts on an outdoor market zone and an indoor part inside the *Bucur Obor*, a large commercial building that has been parceled up into hundreds of small, independent retail stores. The *Obor Market* is thus a crowded place every day with people coming from outside the capital city to sell their products in the market area and the inhabitants of Bucharest coming to purchase their daily groceries.

Figure 8 *Obot Market* Area for Trial

This area is also an important hub in city transportation as in the vicinity converge a subway station, a tramway station and bus stations. In the same time, the area has also facilities for leisure time in the *Obor Park* area which is transformed into an ad-hoc market during Christmas and Easter.

However, the area is known also for its illegal activities among which the most prominent are:

- drugs trafficking,
- theft,
- illegal cigarettes trafficking,
- illegal street trading,
- pick-pocketing etc…

For this reason, Bucharest City Sector 2 Council has tried to reduce the criminality in the area increasing the Police patrols but slight differences have been perceived. According to recently citizens' surveys, *Obor* area is considered as one of the most unsecure areas in Bucharest and the people and shop keepers' communities perceive it as a constant source of insecurity and violence. Mayor's Office together with the Local Police Department started in 2009 to install cameras in the main intersections and streets and decreased the number of illegal activities notoriously together with an improvement of the public perception of safety.

6.4.2 Potential infrastructures to be used

Bucharest Sector 2 City Council provides a complex and diverse testing ground for several applications. The experimentation facilities imply a surveillance network made up of cameras and sensors and located in buildings, and lampposts connected via optical fiber to an access point used to send the signal to the existing Command and Control Centre. This C2 centre will have internet broadband connectivity to access on-line functionalities. In addition, Mobile Police Patrol Units, Police Patrol Cars and citizens will make use of 3G connectivity to internet to enable the usage of SafeCity capabilities.

On the other hand, Bucharest Sector 2 City Council has already in place a command and control centre for the 100 cameras deployed in the Sector 2 area and will provide enough room for the installation and running of the needed servers and desktops.

6.4.3 Communities involved

During Phase 2, SafeCity will count on the real involvement of Bucharest Sector 2 City Council. Moreover, it is planned to have a public awareness campaign in order to provide the general public the information about the project. It is expected that, once the pilot is running, citizens will actively participate and use the reporting and notification applications.

6.4.4 Ethical and Legal Framework

SafeCity has already performed a detail analysis of the ethical and legal aspects of deployment of a video-surveillance system in Bucharest.

In Romania, the processing of video data in the context of protection of personal data is regulated by Law No. 677/2001 on the "Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, amended and completed" and Decision no. 52 of 31st of May 2012 regarding the processing of personal data obtained via video surveillance.

7. Definition of experimentation infrastructure for Phase 2

This section aims to define the experimentation infrastructure to develop in Phase 2 for those pre-selected test-beds. Particularly, it is intended to describe what and how the R&D Technologies defined in the Section 4 can be tested in those pre-selected test-beds.

For this purpose, the concept of "*SafeCity Case Study*" defined in the deliverable D3.2 is used again. As already explained in D3.2, "*A SafeCity Case Study is a composite element describing a use case of the SafeCity technology in one or more reference context plus expresses its functionality in terms of aggregation of applications in a standardized way. It implies both an in-depth description of its technical components and its end-user aspects and is used for validation of concepts, technologies and user aspects*" and it is also composed of two different levels:

- The Application level consists of the applications (or R&D technologies) that provide the technology foundations for the operation of Case Studies.
- The Enablers level consists of the Enablers that compose the building blocks of the applications and may be provided by FI-WARE (Generic Enablers) or by SafeCity (Specific Enablers).

However, unlike the work performed in D3.2 where the SafeCity Phase 2 Public Safety Case Studies were composed of Phase 1 SafeCity applications and further Public Safety applications defined in the deliverable D2.8, at this stage the Phase 2 Case Studies are going to be composed of the R&D Technologies (or Applications) that have been presented in the Section 4.

7.1 Phase 2 Case Studies

As already known, the SafeCity Phase 2 Public Safety Case Studies defined in D3.2 were the following ones:

- Enhanced detection and tracking of a suspicious citizen
- Early detection of a suspicious abandoned backpack in a public space and subsequent evacuation order
- Early detection and response for critical changes in road condition
- Early detection of an environmental incident
- Intelligent and trustworthy management of large events

Since a complete analysis for these Phase 2 Case Studies has already been carried out, at this stage it is only going to be explained what and how the R&D Technologies (Applications) are going to be involved in the different Case Studies in order to be tested in the pre-selected test-beds.

7.1.1 Case Study 1: Enhanced detection and tracking of a suspicious citizen

This Phase 2 Case Study aims to detect a suspicious person by either his/her suspicious activities, his/her detected identity or both, based also on prior data and proper modelling of person identities with respect to facial features and suspicious movement patterns associated with loitering, and then, to track such suspicious person in much more complex situations, as for example, the tracked person disappears from the view of the cameras.

For this purpose, this Case Study must be composed of applications which enable the early detection of suspicious people based on advanced video processing from authorities surveillance cameras, intelligent analytics techniques for automated detection, advanced tracking and monitoring of the suspicious person and cross-checking with other information sources. In addition, this Case Study must be also complemented by applications which allow secure communications and data privacy and provide monitoring and evaluations tools in order to evaluate the performance of all Applications.

Below, it is summarized what and how Applications will take part of this Phase 2 Case Study.

APPLICATIONS	ROLE
APP1: Sensors Activation, Control and Information Enablement	It will handle activation, configuration, connectivity and control of surveillance cameras.
APP2: Heterogeneous Data Aggregation and Pre-processing	It will tackle aggregation of data from different surveillance cameras in a synchronized manner.
APP3: Scalable Multimedia Analytics, Multimodal Fusion	It will analyze simultaneously streamed multimedia data from surveillance cameras. It will also perform video analysis and processing, pattern recognition algorithms to produce low and middle-level detection results, fed to multimodal fusion techniques to account both for higher accuracy in detection and higher semantics infering.
APP4: Heterogeneous Data Streaming and Storage	It will provide core storage and distribution facilities in multimedia content and information workflows for other Applications.
APP5: High Level Data Fusion & Reasoning, Semantic Information Management	It will fusion incoming data and relate them to other events where the suspicious person is involved.
APP6: Decision Support System	It will allow to alert public safety personnel on detected suspicious people (from APP5) and to assist decisions for action. It will use the following functionalities: - decision support system; - messaging/alerting; - interactive/intuitive UI; - operator feedback to Video Analytics; - 3D positioning and tracking;
APP8: Communication and Data Security, Privacy Control	It will provide secure communications and ensure data privacy. Also, it will manage security aspects of all Applications in this Case Study.
APP10: Performance Monitoring and Evaluation Tools	It will provide monitoring and evaluation tools for tests in order to objectively evaluate the performance of all APPs within the Case Study.

Table 5 Applications involved in Phase 2 Case Study 1

7.1.2 Case Study 2: Early detection of a suspicious abandoned backpack in a public space and subsequent evacuation order

This Phase 2 Case Study aims to detect a potentially suspicious abandoned backpack (orphan/left object) to prevent any potential terrorist attack or criminal act in public spaces. The detection is facilitated by analysing multiple camera feeds in the monitored city area and detecting any moving objects in any of these camera feeds.

For this purpose, this Case Study must be composed of applications which enable the early detection of suspicious abandoned backpack based on advanced video processing from authorities surveillance cameras, intelligent analytics techniques for automated detection, cross-checking with other information sources and dispatch of emergency messages for the evacuation order. In addition, this Case Study must be also complemented by applications which allow secure communications and data privacy and provide monitoring and evaluations tools in order to evaluate the performance of all Applications.

Below, it is summarized what and how Applications will take part of this Phase 2 Case Study.

APPLICATIONS	ROLE
APP1: Sensors Activation, Control and Information Enablement	It will handle activation, configuration, connectivity and control of surveillance cameras.
APP2: Heterogeneous Data Aggregation and Pre-processing	It will tackle aggregation of data from different surveillance cameras in a synchronized manner.
APP3: Scalable Multimedia Analytics, Multimodal Fusion	It will analyze simultaneously streamed multimedia data from surveillance cameras. It will also perform video analysis and processing, pattern recognition algorithms to produce low and middle-level detection results, fed to multimodal fusion techniques to account both for higher accuracy in detection and higher semantics infering.
APP4: Heterogeneous Data Streaming and Storage	It will provide core storage and distribution facilities in multimedia content and information workflows for other Applications.
APP5: High Level Data Fusion & Reasoning, Semantic Information Management	It will fusion incoming data and relate them to other events which hint the same incident.
APP6: Decision Support System	It will allow to alert public safety personnel on detected suspicious people (from APP5) and to assist decisions for action. It will use the following functionalities: - decision support system; - messaging/alerting;

	- interactive/intuitive UI; - operator feedback to Video Analytics;
APP7: Communities Involvement & UG Content Management System	It will allow to send alert notifications to citizens located in the area to be evacuated with the aim of performing a quick evacuation.
APP8: Communication and Data Security, Privacy Control	It will provide secure communications and ensure data privacy. Also, it will manage security aspects of all Applications in this Case Study.
APP10: Performance Monitoring and Evaluation Tools	It will provide monitoring and evaluation tools for tests in order to objectively evaluate the performance of all APPs within the Case Study.

Table 6 Applications involved in Phase 2 Case Study 2

7.1.3 Case Study 3: Early detection and response for critical changes in road condition

This Phase 2 Case Study aims to detect early the changes in road condition and to alert citizens, officials or the police about the possible changes in travel conditions.

For this purpose, this Case Study must be composed of applications which enable the early detection of alerting situations caused by vehicles, traffic, etc. mainly based on advanced video processing from the existing traffic video surveillance systems, on information processing from different types of sensors and on information processing generated by citizens. In addition, this Case Study must be also complemented by applications which allow secure communications and data privacy and provide monitoring and evaluations tools in order to evaluate the performance of all Applications.

Below, it is summarized what and how Applications will take part of this Phase 2 Case Study.

APPLICATIONS	ROLE
APP1: Sensors Activation, Control and Information Enablement	It will handle activation, configuration, connectivity and control of traffic cameras and environmental sensors.
APP2: Heterogeneous Data Aggregation and Pre-processing	It will tackle aggregation of data from different traffic cameras in a synchronized manner, as well as sensor data preprocessing in real-time at gateway devices.
APP3: Scalable Multimedia Analytics, Multimodal Fusion	It will analyze simultaneously streamed multimedia data from traffic cameras. It will also perform video analysis and processing, pattern recognition algorithms to produce low and middle-level detection results, fed to multimodal fusion techniques to account both for higher accuracy in detection and higher semantics infering.
APP4: Heterogeneous Data Streaming and Storage	It will provide core storage and distribution facilities in multimedia content and information workflows for

	other Applications.
APP5: High Level Data Fusion & Reasoning, Semantic Information Management	It will fusion incoming data from traffic cameras, environmental sensors and citizens into higher level constructs and relate them to other alerting situations.
APP6: Decision Support System	It will allow to alert public safety personnel on alerting situations caused by vehicles, traffic, etc. (from APP5) and to assist decisions for action. It will use the following functionalities: - decision support system; - sensors/processing triggers; - messaging/alerting; - interactive/intuitive UI;
APP7: Communities Involvement & UG Content Management System	It will enable the involvement of communities in public safety, such that the citizens can send media emergency messages and receive alert notifications related to critical changes in road condition. In addition, the UG Content Management System will be used for filtering user generated content in this Case Study.
APP8: Communication and Data Security, Privacy Control	It will provide secure communications and ensure data privacy. Also, it will manage security aspects of all Applications in this Case Study.
APP10: Performance Monitoring and Evaluation Tools	It will provide monitoring and evaluation tools for tests in order to objectively evaluate the performance of all APPs within the Case Study.

Table 7 Applications involved in Phase 2 Case Study 3

7.1.4 Case Study 4: Early detection of an environmental incident

This Phase 2 Case Study aims to detect in near real-time environmental incidents and provide early warning to the citizens and the responsible bodies and authorities to act immediately and consequently to minimize the property and human lives loss.

For this purpose, this Case Study must be composed of applications which enable an efficient collection and analysis of relevant environmental data that is overlaid with other surveillance information to jointly generate new potential positive alerts. In addition, it must be allowed that authorities as well as volunteering citizens can also inform about environmental incidents. Moreover, this Case Study must be also complemented by applications which allow secure communications and data privacy and provide monitoring and evaluations tools in order to evaluate the performance of all Applications.

Below, it is summarized what and how Applications will take part of this Phase 2 Case Study.

APPLICATIONS	ROLE
APP1: Sensors Activation, Control and Information Enablement	It will handle activation, configuration, connectivity and control of environmental sensors.
APP2: Heterogeneous Data Aggregation and Pre-processing	It will allow environmental sensor data preprocessing in real-time at gateway devices.
APP4: Heterogeneous Data Streaming and Storage	It will provide core storage and distribution facilities in multimedia content and information workflows for other Applications.
APP5: High Level Data Fusion & Reasoning, Semantic Information Management	It will fusion incoming environmental data into higher level constructs and perform cross-checking of input data
APP6: Decision Support System	It will allow to alert public safety personnel on environmental incidents (from APP5) and to assist decisions for action. It will use the following functionalities: - decision support system; - messaging/alerting; - sensors/processing triggers; - interactive/intuitive UI;
APP7: Communities Involvement & UG Content Management System	It will enable the involvement of communities in public safety, such that the citizens can send media emergency messages and receive alert notifications related to environmental incidents. In addition, the UG Content Management System will be used for filtering user generated content in this Case Study.
APP8: Communication and Data Security, Privacy Control	It will provide secure communications and ensure data privacy. Also, it will manage security aspects of all Applications in this Case Study.
APP10: Performance Monitoring and Evaluation Tools	It will provide monitoring and evaluation tools for tests in order to objectively evaluate the performance of all Applications within the Case Study.

Table 8 Applications involved in Phase 2 Case Study 4

7.1.5 Case Study 5: Intelligent and trustworthy management of large events

This Phase 2 Case Study aims to manage and control large events like organized events or spontaneous social events that are not foreseen by public authorities, and where critical changes on the roads, overcrowding of people, suspicious citizen behaviour, etc. can occur.

For this purpose, this Case Study must be composed of applications which enable the early detection of suspicious people based on advanced video processing from authorities surveillance cameras, the early detection of alerting situations caused by vehicles, traffic, etc., information processing generated by

citizens, intelligent analytics techniques for automated detection, cross-checking with other information sources and dispatch of emergency messages for the evacuation order. In addition, this Case Study must be also complemented by applications which allow secure communications and data privacy and provide monitoring and evaluations tools in order to evaluate the performance of all Applications.

Below, it is summarized what and how Applications will take part of this Phase 2 Case Study.

APPLICATIONS	ROLE
APP1: Sensors Activation, Control and Information Enablement	It will handle activation, configuration, connectivity and control of surveillance cameras, traffic cameras and environmental sensors, if needed.
APP2: Heterogeneous Data Aggregation and Pre-processing	It will tackle aggregation of data from different surveillance and traffic cameras in a synchronized manner.
APP3: Scalable Multimedia Analytics, Multimodal Fusion	It will analyze simultaneously streamed multimedia data from surveillance and traffic cameras. It will also perform video analysis and processing, pattern recognition algorithms to produce low and middle-level detection results, fed to multimodal fusion techniques to account both for higher accuracy in detection and higher semantics infering.
APP4: Heterogeneous Data Streaming and Storage	It will provide core storage and distribution facilities in multimedia content and information workflows for other Applications.
APP5: High Level Data Fusion & Reasoning, Semantic Information Management	It will fusion incoming data and correlate them to other situations which are related to the large event
APP6: Decision Support System	It will allow to alert public safety personnel on detected suspicious people, situations caused by traffic, overcrowding of people, etc. (from APP5) and to assist decisions for action. It will use the following functionalities: - decision support system; - sensors/processing triggers; - messaging/alerting; - interactive/intuitive UI; - operator feedback to Video Analytics;
APP7: Communities Involvement & UG Content Management System	It will enable the involvement of communities in public safety, such that the citizens can send media emergency messages and receive alert notifications related to environmental incidents. In addition, the UG Content Management System will be used for

	filtering user generated content in this Case Study.
APP8: Communication and Data Security, Privacy Control	It will provide secure communications and ensure data privacy. Also, it will manage security aspects of all Applications in this Case Study.
APP10: Performance Monitoring and Evaluation Tools	It will provide monitoring and evaluation tools for tests in order to objectively evaluate the performance of all APPs within the Case Study.

Table 9 Applications involved in Phase 2 Case Study 5

7.2 Test Definition

7.2.1 Madrid Test-bed

Tests in the Madrid test-bed will mainly rely on the advanced video surveillance system located in AZCA, and in addition, on the following Command and Control Centres:

- Lightening and Access Galleries Control Centre of Madrid Municipality,
- CISEVI (Integrated Video Signal Center), and
- CISEM (Integrated Centre of Emergencies in Madrid)

Besides, mobile 3G devices will be also used to provide surveillance information to the system.

From these infrastructures, the Phase 2 Case Studies that could be tested with all its applications are the following ones:

- Enhanced detection and tracking of a suspicious citizen
- Early detection of a suspicious abandoned backpack in a public space and subsequent evacuation order

Additionally, certain functionalities of APP7 - Communities Involvement & UG Content Management System could be also tested.

7.2.2 Athens Test-bed

Tests in the Athens test-bed will mainly rely on the traffic video surveillance system located in different places of the city, and on the Athens Traffic Management Centre (ATMC).

Therefore, these infrastructures will provide facilities the testing of the following Phase 2 Case Studies:

- Early detection and response for critical changes in road condition

Additionally, certain functionalities of APP7 - Communities Involvement & UG Content Management System could be also tested.

7.2.3 Turin Test-bed

Tests in the Turin test-bed aim to enhance the safety of the citizens. The areas for safety to be considered are:

- bicycle parking facilities,
- outdoor local market areas,

- public urban green spaces,
- outdoor meeting spaces,
- public transport system, and
- public parking lot.

For this purpose, tests will mainly rely on the smart public lighting system and the cameras with local storage located in the areas considered. In addition, control infrastructure and Police Station premises in the area will be also used.

From these infrastructures, the Phase 2 Case Studies that could be tested with all its applications are the following ones:

- Enhanced detection and tracking of a suspicious citizen
- Early detection of a suspicious abandoned backpack in a public space and subsequent evacuation order
- Early detection and response for critical changes in road condition
- Early detection of an environmental incident
- Intelligent and trustworthy management of large events

7.2.4 Bucharest Test-bed

Tests in the Bucharest test-bed will mainly rely on the advanced video-surveillance system located in the Sector area and managed by a command and control centre located in the same place.

In addition, Mobile Police Patrol Units, Police Patrol Cars and citizens will make use of 3G connectivity to internet to provide surveillance information to the system.

From these infrastructures, the Phase 2 Case Studies that could be tested with all its applications are the following ones:

- Enhanced detection and tracking of a suspicious citizen
- Early detection of a suspicious abandoned backpack in a public space and subsequent evacuation order

Additionally, certain functionalities of APP7 - Communities Involvement & UG Content Management System could be also tested.

8. Assessment of Phase 2 success

Thanks to the success achieved in Phase 1, SafeCity assets different methods to reach further success in future phases (First of all for FI-PPP Phase 2 and then Phase 3).

It is important to highlight that SafeCity was the first use case using FI-WARE test-bed platform and its connectivity, being an important action within FI-PPP.

During the test, all SafeCity applications worked as expected:

1. Applications running on the FI-WARE test-bed in Seville, Spain:
    a. **Rule Based Engine**, using the CEP GE, processed incoming events
    b. **Data Fusion**, running on a Virtual Machine on the test bed and using the SAS GE, further stored and semantically processed the information
    c. **Decision Support System**, running on a Virtual Machine on the test bed delivered the User Interface over the internet to browsers in the command centers
2. Applications running locally in Stockholm:
    a. **Sensors and Sensor Adapters** collected environmental data
    b. **Ad Hoc radio network** transmitted the data to the Gateways
    c. **Gateways** collected the sensor data and made it available for processing on the FI-WARE test bed
    d. **Security manager** securely transferred the data from the Sensor Adapters to the Gateways.

This milestone was considered one of the main success points of SafeCity and this fact may be reflected in the future of SafeCity (Phase 2). In this sense, part of the current consortium of SafeCity, together with other new partners have been hardly working to take part of the Phase 2 of FI-PPP with the new project called “SafeCity2”.

Since the possibility of participating in the Phase 2 of FI-PPP is not completely certain, other possibilities have been set up in order to achieve the success of SafeCity concept in Phase 2 :

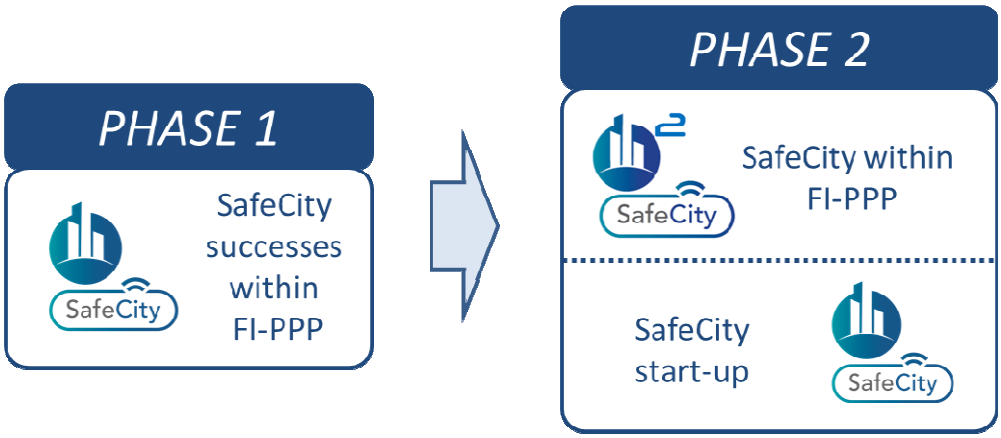


Figure 9 Possibilities to achieve the success of SafeCity concept in Phase 2

8.1 SafeCity belonging FI-PPP:

Together with FI-WARE, INFINITY, CONCORD and other four use cases. In this Phase 2, SafeCity (now called ***SafeCity2***) aims to continue the work initiated in Phase 1, with the focus on the area of the Public Safety and Security making smart public areas safer.

The ultimate challenge of SafeCity2 project is to significantly advance the implementation and uptake of Future Internet services in the area of Public Safety by 2015, leveraging the Internet infrastructure as the basis of user-centred open innovation schemes.

SafeCity2 will also pave the way to run large-scale trials for Phase 3 at time that will increase the involvement of SMEs in the area of the Public Safety.

All these activities will be aligned with the strategic objectives of the FI-PPP programme and the on-going progress there.

One of the main objectives of the project in Phase 2 is the involvement of end users and SME's, the cooperation and exchange of information, for this reason, some actions will be taken. Three different communities will be created to join interest, needs and feedback. Those Communities will be split according with the involvement category:

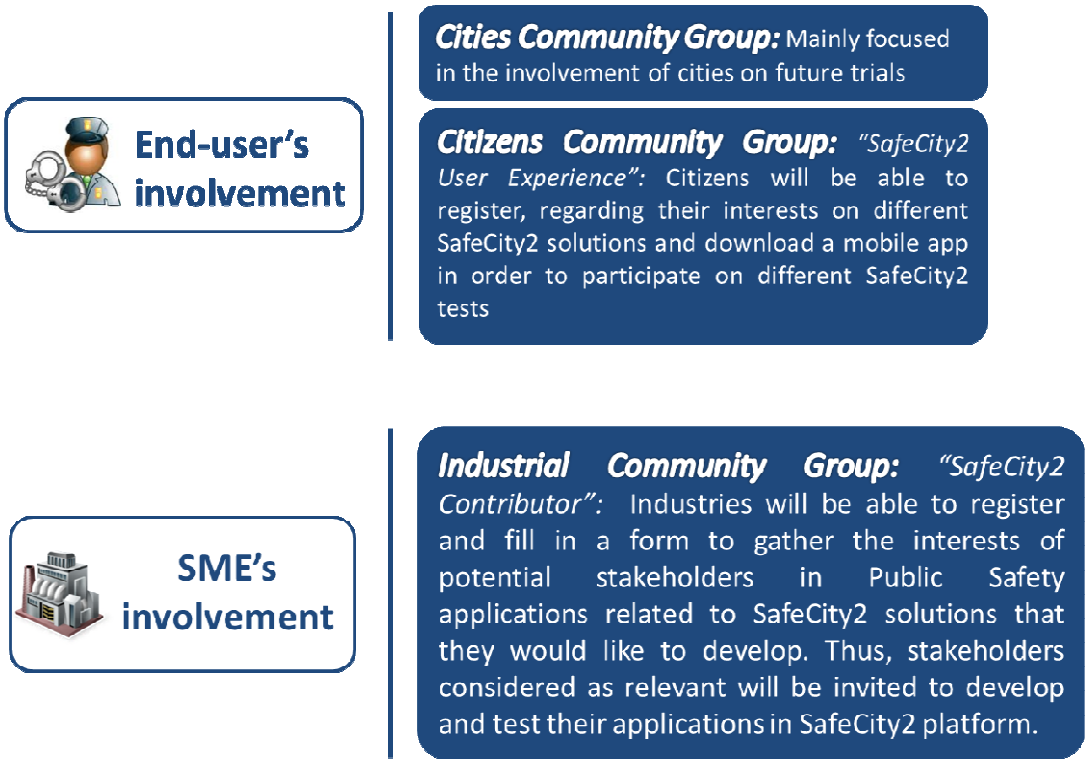


Figure 10 Involvement of end users and SME's and Communities Group

Another important objective of SafeCity2 project in the Phase 2 is the quick and deepest implementation in the market, using new methods and applications. The commercialization strategy of SafeCity2 solution will be explored in two main areas:

- As part of FI-PPP solution (taking in consideration FI-WARE Core Platform, Use Cases potential commercial interaction, etc.)
- As independent entity (*SafeCity2 start-up* – see section 9.2)

SafeCity exploitation strategy will identify different commercial relationships among the different target groups of stakeholders as shown in the chart attached (Business & Exploitation Model Map).

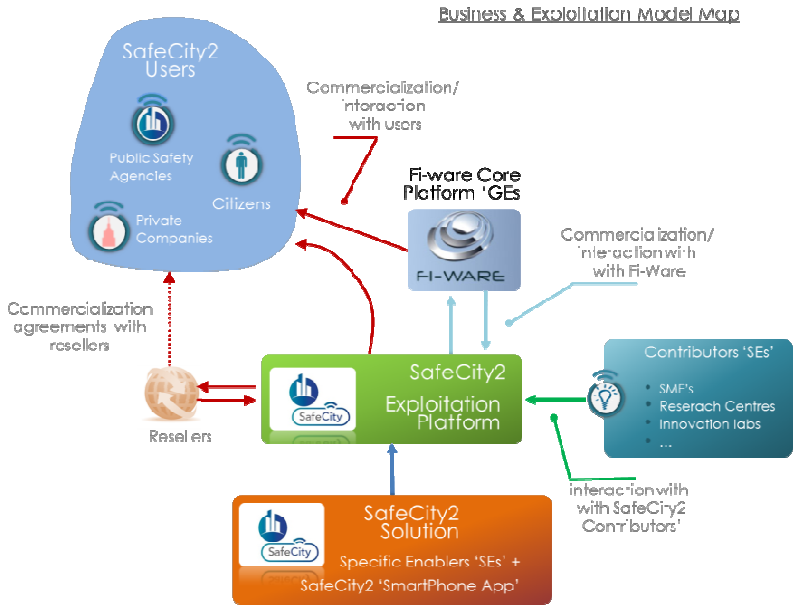


Figure 11 Business & Exploitation Model Map

This map will try to explain in a glance the exploitation and implementation strategy taken by SafeCity2 together with FI-WARE and also through its own "SafeCity2 Exploitation Platform", which will be able to work alone or in accompanied of FI-WARE Core Platform.

As represented in the map, other methods will be used to implement the solution into the market (Resellers, Stakeholders, partners, etc.)

8.2 SafeCity start-up:

The creation of this start-up will be the alternative versus the continuation within FI-PPP in Phase 2. This may be due to the rejection of SafeCity2 into the Phase 2 of FI-PPP or also for other technical and economic reasons.

Once took this mean, two different alternatives are planned:

- **SafeCity with FI-WARE**: FI-WARE's Generic Enablers may be used by SafeCity solution though several contracts between FI-WARE and SafeCity start-up. Also FI-WARE Core Platform services may be hired in order to support the go-to-market phase of SafeCity. In this case, SafeCity will count with FI-WARE components and support though several contracts, which must be detailed during the agreements.
- **SafeCity self-reliant**: This start-up will work with SafeCity as a standalone solution, independent from FI-PPP and FI-WARE Generic Enablers. In this sense, also SafeCity implementation and exploitation will be carried out by SafeCity, without the support of FI-WARE Core Platform.

All SafeCity current partners will be free to join the start-up. Thus, in this sense, SafeCity start-up would have experience, skills and knowledge of working with people to give their potential clients the best customer service they have ever experienced.

Because SafeCity business will be young among the market, the key to success developing market share involve the ability to deliver service quickly and reliably, and to scale operations quickly without loss of quality.

This strategy offers several advantages which make it attractive to sell the products; one of the main advantages is that by using this distribution channel all the trade margin of the operation can be taken by the start-up company. The absence of intermediaries in the sale ensures that the final price paid by the end users is net income for the company, thereby increasing the profitability associated.

Currently a sales operation plan is being developed within the deliverable *D8.2- Exploitation Plan and Business Model*, where sales and operation strategies are detailed and developed. According with the D8.3, sales will operate based in two channels, on one hand, sales through intermediaries and on the other hand, direct sales to end users. To centralize all operation and distributions, a first office must be set up during first year, with the intention of set up more according with the success of SafeCity start up and market needs.

The chart provided below describes the proposed activity to be carried out by SafeCity start up once project is ended. In summary, following illustrative graphic shows SafeCity evolution after the end of the project.

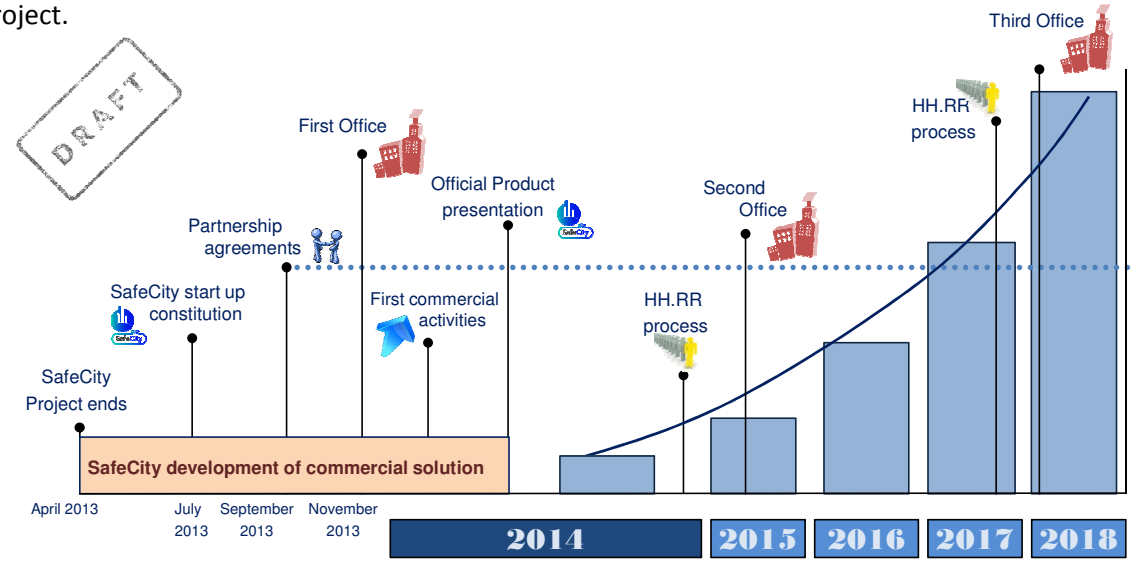


Figure 12 SafeCity evolution after the end of the project

According with the chart above, SafeCity start-up shall be set up as soon as SafeCity Project finalizes, bearing in mind the alternative of SafeCity2 together with FI-PPP. In case that SafeCity2 does not success within the Phase 2 of FI-PPP, the possibility of SafeCity start-up will jump immediately.

Although SafeCity2 does not go through the Phase 2 of FI-PPP, and SafeCity set up a self-reliant start-up, The SafeCity Exploitation Platform (Detailed in Section 9.1) must be also developed. In order to perform said platform, the new start-up will look for public and private funding, both including new partners to the new start-up or creditors.

In this sense, SafeCity solution will count with the support of the exploitation platform for the go-to-market strategy, where stakeholder, resellers and end-user will be involved. This platform connects the market with the company and all the bodies related involve in the implementation and market in a transparent way for both, seller and consumer.

SafeCity exploitation platform brought up for the Phase 2 of FI-PPP includes FI-WARE exploitation platform within its components, as other additional body to connect. This new platform established for

SafeCity out of FI-PPP, may also count with the support of FI-WARE platform or work self-supported (In case FI-WARE collaborate with SafeCity Platform, each relationship must be reflected in a legal agreement).

Pros and Cons of setting up SafeCity start-up

Deciding to set up a new SafeCity start-up was analyzed and evaluated through different studies, like PEST and SWOT analyses. As result of SWOT analysis, several advantages and disadvantages have been detected, and detailed below:

Strengths: The biggest strength of this Project is the high innovative component service, besides the low competiveness that we can find in the market, owing to the ability of adaptability of the product (with all its versions).

This consortium has had the capacity to see a market niche in one of the latest sectors, the Smart Cities. As well as providing to the market with different solutions adaptable to the conditions and needs of the costumer.

Weakness: One of the SafeCity start-up's weakness is the accessibility to key distribution partners, which will deal with the commercialization of SafeCity in an international level, allowing a greater

Also an important need of investment for all the partners in order to achieve the constitution of a company which commercialize the product may be necessary. Having into account that it is important to point out the existence of a huge crisis situation throughout which involves that some partner might not enjoy of the financial resources to face the sale, this may cause an important budget constriction.

Opportunities: Although there are competitors, the market is covering if we break the concept down, but in this moment there are not a great number of companies which provide an integrated solution.

By analysing the external environment and SafeCity internet environment, it is possible to think about future strategies in a short term.

Threats: There is a great capacity to imitate the products framing in the security and ICT markets, becoming an important risk that the consortium will have into account at the moment OF defining the strategy of sales. This strategy will have into account that the economic public institutions are situated in a crisis period, and therefore its budget is being drastically reduced.

Taking in consideration this analysis, the implementation of SafeCity on the market as a start-up seems to be a good option.

In order to sum up different alternatives proposed by SafeCity in the Phase 2 of the project, following chart has been created:

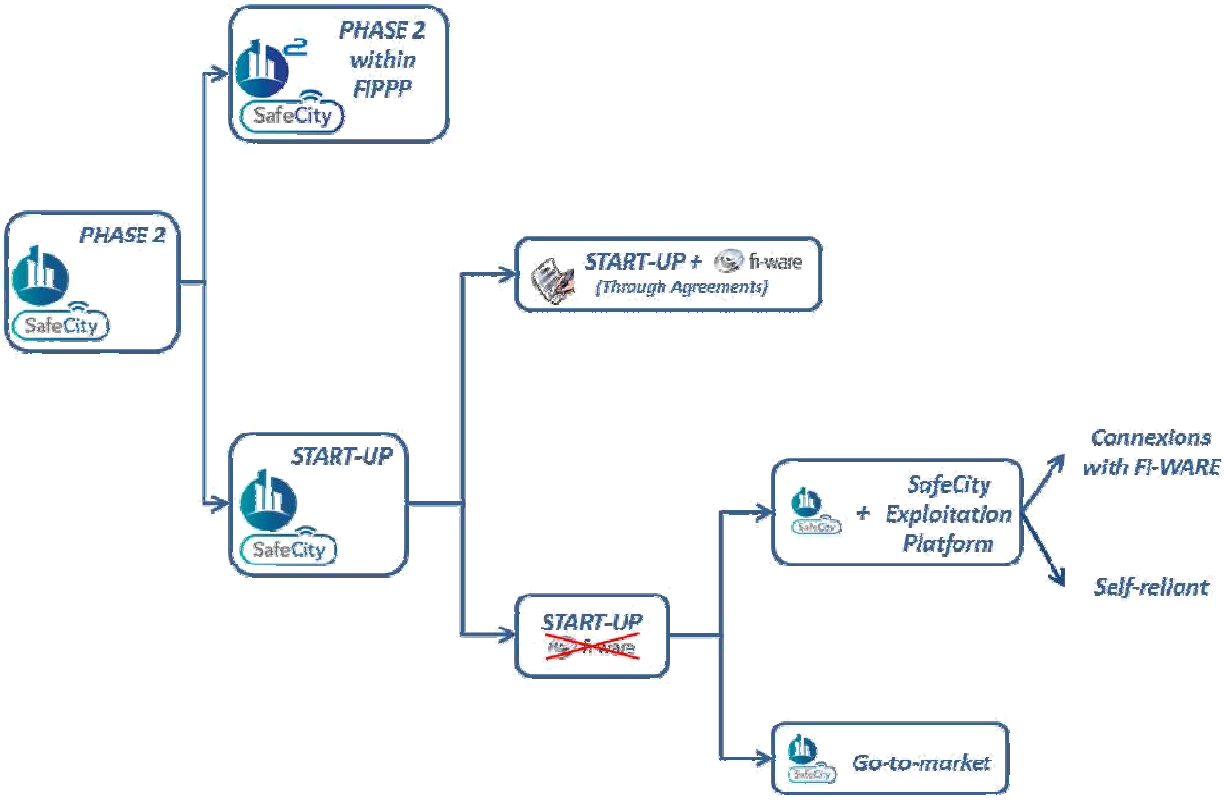


Figure 13 Different alternatives proposed by SafeCity in the Phase 2 of the project