FP7-285556 SafeCity Project

Deliverable D2.8

Title: Specific Enablers on Public Safety in Smart Cities

Deliverable Type:	**CO**
Nature of the Deliverable:	**O**
Date:	**27/10/2011**
Distribution:	**WP2**
Editors:	**ARATOS**
Contributors:	**ISD, AIT, TEK, ATH, HIB, MCC, MIT, TIL, VTT, FOI, KEM, THA, 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 serves as a summary of the enablers defined in Public Safety in Smart Cities

DISCLAIMER

The work associated with this report has been carried out in accordance with the highest technical standards and SafeCity partners have endeavored 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
ARA	Myrto Zacharaki, Giorgos Kostopoulos
ISD	Diego Giménez, Judith Pertejo
AIT	Tassos Dimitriou, Sofia Tsekeridou
TEK	Pedro Antonio
ATH	Peretz Gurel, Gabriel R. Feldman
HIB	Roberto Giménez, Emilio Martin
FOI	Anders Hansson, Jan Nilsson
THA	Sophie Chague, Christophe Meyer
TEN	Francisco Ruiz

Document History

Date	Version	Editor	Change	Status
20110625	0.1	Myrto Zacharaki Giorgos Kostopoulos	First Draft of D2.8 deliverable template	Draft
20110722	0.2	Myrto Zacharaki Giorgos Kostopoulos	Overview of work organization, definition of enablers and descriptions	Draft
20110725	0.3	Myrto Zacharaki Giorgos Kostopoulos	Updated table of contents	Draft
20110729	0.4	Myrto Zacharaki Giorgos Kostopoulos	Initial enablers definition	Draft
20110826	0.5	Myrto Zacharaki Giorgos Kostopoulos	Update in the methodology of enablers definition Reference to FIWARE GE enablers Organization of contributions	Draft
20110823	0.6	Myrto Zacharaki Giorgos Kostopoulos	Updated new contributions Final corrections Preparation for internal assessment	Prefinal
20111010	0.7	Myrto Zacharaki Giorgos Kostopoulos	Further contributions and corrections edited	Prefinal
20111021	0.8	Myrto Zacharaki Giorgos Kostopoulos	Final integration of partners' inputs and Final corrections in presentation according to the official deliverable format	Prefinal – Sent for internal review
20111027	0.8	Judith Pertejo Lopez	Internal Review Comments	Prefinal – Commented and reviewed internally
20111027	0.9	Myrto Zacharaki Giorgos Kostopoulos	Final corrections based upon internal reviewer's comments	Final version to be submitted

Table of Contents

List of Figures

List of Tables

Glossary

Acronym	Meaning
PS	Public Safety
UC	Use Case
CP	Core Platform
CP	Civil Protection
ICT	Information & Communication Technology
MANET	Mobile Ad-hoc Network
C2	Control & Command Center
M2M	Machine-to-Machine
GPS	Global Positioning System
QoS	Quality of Service

References

Number	Reference
[1]	FIWARE High-Level Description (Product Vision), version 11-08-1
[2]	SafeCity D3.1 Specific Requirements Definitions
[3]	SafeCity D7.1 Social, Ethical & Legal Implications
[4]	SafeCity D7.2 SafeCity Policy Making
[5]	SafeCity D2.7 Public Safety Scenarios guidelines and conclusions
[6]	SafeCity D2.1 Madrid Public Safety Scenario
[7]	SafeCity D2.2 Bucharest Public Safety Scenario
[8]	SafeCity D2.3 Athens Public Safety Scenario
[9]	SafeCity D2.4 Stockholm Public Safety Scenario
[10]	SafeCity D2.5 Helsinki Public Safety Scenario
[11]	SafeCity D2.6 Obidus Public Safety Scenario
[12]	A. Magkanaraki, G. Karvounarakis, T. Anh, V. Christophides, D. Plexousakis, Ontology Storage and Querying, Technical Report No 308, Foundation for Research and Technology, Hellas Institute of Computer Science, Information Systems Laboratory, April 2002

1. Introduction

1.1 Specific and Generic Enablers

The current document presents the set of functionalities found necessary in Public Safety Use Cases [5]. Following FIWARE's descriptions upon enablers [1], functionalities are being organized in blocks forming the Public Safety enablers. Each enabler serves a set of key functionalities in its area and it may be adapted to several case scenarios as necessary.

The work presented shall overview both Generic and Specific enablers related to Public Safety operations. The first have been defined by FIWARE in [1] and present the functional requirements related to the Core Platform operation and architecture, i.e. covering generic features of Future Internet capabilities to be undertaken by the respective users and providers involved, in various usage areas. Similarly, the second describe the set of functional capabilities found in Public Safety scenarios. In this case, specific implies that the related functionalities appear to have no applicability (and thus significance) in other Use Cases and so their scope is limited to the description of Public Safety use cases.

The research conducted has received valuable inputs from the SafeCity's involved end-users, through an assembly of brief questionnaires, the findings of which were presented in the End-Users Workshop organized by SafeCity in September, 2011 [5], as well as through a study of the involved cities studied and their respective Public Safety operational scenarios [6-11]. The information received included functional requirements in the level of the sensors, communication infrastructures, human-intervention, system evaluation, etc as well as ethical and legal constraints related to sensitive data and their protection under constitutional laws.

The current study focuses on the functional requirements of the Public Safety Use cases and the description of the capabilities of the enablers required in response to them. In the current form of our presentation, both the Generic and the Specific enablers' definitions are in progress. Definitions of Generic Enablers have been corresponded to the four areas of Public Safety Use Case (see below in Section 1.2), and additional Specific Enablers have been defined to fulfill potential gaps. Looking into future more detailed descriptions of the Generic enablers' capabilities and at accordingly additional capabilities for Specific enablers, the current research will be developed and updated accordingly.. Therefore, the description of the Specific enablers is not fulfilled and continuously extra input information is received to determine their functions completely.

Additionally, the current research examines high level descriptions of the functional requirements of the components needed to be realized for the Public Safety Use Case. Parallel development in SafeCity's deliverable D3.1 [2] examines in more detail the specific features and operational (technical) requirements of these descriptions.

1.2 Public Safety Functionalities

Public Safety Use Cases are being realized, or otherwise enabled, by the introduction of a set of functionalities. These are found across the different operational levels of related applications and they describe key providers', users' and stakeholders' requirements. Under this context, we expect definitions of functionalities to look into the expected *behaviors* founded across interrelated technical development, business considerations, ethical and legal constraints, etc.

Applications, and thus functionalities, in Public Safety Use cases can be classified upon the following four categories:

- **Situational Awareness;** obtained by the deployment of sensor technologies on the areas of interest
- **Ad-Hoc Networks**; ensuring complete and reliable network support independent of temporal and spatial variations
- **Command and Control Centers (C2);** Storing, assessing and managing the data received, defining response actions upon them
- **Alerting technologies;** Transferring C2 commands on response strategies to Civil Protection members on the field, other Public Safety organizations, etc

These constitute the main phases of Civil Protection engineering and the primary high-level categorization of processes and behaviors. Further analysis to the above, can lead us to the more specific applications and services found on lower level. **Table 1** presents an example overview of such analysis:

Situational Awareness	Ad-Hoc Networks
1. Surveillance – deployed sensors with sufficient area coverage and ability to monitor defined features/ situations/ etc *1.1. Dynamic Surveillance* – ability to alter sensors' operational parameters on demand *1.2. Scalable Surveillance* – ability to expand and integrated sensor network **...** **2. Detection** – intelligent algorithms to process and identify abnormalities based on pre-defined parameters *2.1. Abnormal behaviors* *2.2. Abnormal objects* *2.3. Abnormal traffic* ..	**1. Remote network support** – enable communication to areas where no infrastructures are available, via wireless networks *1.1. Heterogeneous network support* **–** ability to connect to existing networks upon the protocols being used ... **2. Moving stations support** *2.1. Mobile C2* *2.2. Mobile units* ...
Control and Command Centers	**Alerting Technologies**
1. Data acquisition – direct and continuous communication with the sensor network deployed **2. Data management and storage** - storing data upon meta-attributes **3. Situation assessment and evaluation –** identification of alerts, types, severity, etc **4. Decision Making –** management of situation based upon nature of alert, available resources, etc to define response strategy	**1. Communication with CP members on the field** **2. Communication with other Public Safety organizations** (e.g. fire departments, CDCs, etc) **3. Communication with citizens** *3.1. SMS alerts* *3.2. Wide screen alerts (e.g. regarding traffic abnormalities, accidents, etc)* *3.3. Viral networks alerts (e.g. Facebook, Twitter, etc)* ....

Table 1 Operational Analysis of the included processes in Public Safety UC

1.3 Capabilities and Requirements

As mentioned above, functionalities are linked to the expected behaviors of the system and in that case they incorporate a holistic overview of technical architectures and capabilities, as well as actors' contributions and demands [5].

The families of actors being involved in the distinct application areas of SafeCity are being considered as displayed in **Table 2** below:

Actor	Monitor	Detect	Send Alert	Data storage	Data MGT	Decision making	Receive Alert	Response
Civil Protection members on the field	✓	✓	✓				✓	✓
Other Public Safety organizations (e.g. fire departments, CDCs, etc)	✓			✓	✓	✓	✓	✓
Citizens			✓				✓	✓
C2 members and Civil Protection experts	✓		✓	✓	✓	✓	✓	✓
Infrastructure and Service Providers	✓	✓	✓					
Application Providers	✓	✓	✓	✓				

Table 2 Analysis of the actors and activities involved in Public Safety UC

Having these in mind, we consider the following in order to define functionalities involved in Public Safety Use Cases operating upon Future Internet architectures:

- **Capabilities introduced in FIWARE (Core Platform)** – these include the set of generic enablers able to provide innovative services to leverage existing applications (applied in all use cases). Main capabilities include among others scalable and flexible architectures, open standards and easy integrations, while additionally support upon the different technical chapters is enabled
- **Users and stakeholders requirements** – these include both description of applications developed so far, which need no change (e.g. criminal databases operating only across private networks), as well as expectations for overcoming major challenges and limitations (e.g. 24/7 support, limited human intervention in C2, interoperability with different Public Safety networks and data formats, etc)
- **Innovative Applications to be introduced (SafeCity Vision**) – these include considerations for optimizing and leveraging existing applications in Public Safety use cases alone (e.g. intelligent real-time video analytics capabilities, advanced QoS delivery upon alerting priorities, etc)

2. Social, Ethical and Legal considerations

While safety and security of public places should be maintained, ethical implications arise in order to guarantee the privacy of citizens. The Public Safety Use Case ultimately makes use of sensitive data, namely

- residence or various geographic recordings, e.g. GPS localization readings
- individual (or collective) day-to-day behavior studies

SafeCity has been exploring regulations and policies on EU and national levels to carefully handle this information, respecting the citizens' constitutional rights. Personal data extracted from surveillance systems should be considered as sensitive data, and therefore subjected to the same constraints. The gathering, processing, storage, transmission, access and visualization procedures of this type of data should comply with ethical European Directives and National Regulations of the EU Member States (see these preliminary ethical requirements in SafeCity's deliverable D2.7 [4]).

Main considerations to be dealt with technically include:

- A physical system protection of sensitive data is required; sensitive databases (criminal records, missing plates, etc.) cannot belong to the public cloud but should be located in secure places as police centers
- Servers that store sensitive databases should be located in a secure domain and database checking should be restricted to highly secure environment, internally; private cloud services need to be set up separately for Public Safety organizations in a way that network resources (computing, storage) are desired not to be shared with other market-oriented services
- Access to sensitive data should be highly restricted to authorized users through password-protection and other mechanisms that guarantee the security requirements; applications that require the sensitive databases requests should be subject to strictest security mechanisms
- A dynamic set up of security levels needs to be implemented where database access, storage and transmission is required; additionally, different encryption levels of storage information and of the transmitted information should be allowed

Such implications are taken under consideration on the definition of the enablers' designs defined below and are also further examined with respect to their legal and ethical frameworks, and supporting policy and management strategies in SafeCity's deliverable D7.1 [3].

3. Situational Awareness

3.1 Introduction

Situational Awareness is a key element in successful Public Safety systems. As the name suggests, the applications, services and infrastructures involved aim in providing holistic and insightful interpretation of the areas being monitored. This extend from the network of sensors deployed being programmable on demand and composed of a various different sources and types (searching for all potential families of threats), to automatically detecting abnormal patterns and ensuring a reliable network support.

End users require that an effective Public Safety system should provide threat detection in the following main areas:

- Citizens behavior – detection of suspicious patterns indicating threats, e.g. an individual staying close to a critical building, such as a bank, for a long time
- Suspicious objects – carrying for the detection of dangerous objects, i.e. objects imported in the area with regard of causing harm, e.g. detecting orphan objects, such as a back-bag found abandoned in a central square
- Traffic-related anomalies – including detection of illegal activities, e.g. crossing to wrong lane, red signal disregards, etc or even malfunctions in traffic – conjunctions, damages in road/ bridge structures, etc
- Environment-related anomalies – detecting anomalies in environmental indicators e.g. particles concentration, etc which could imply a terrorist attack (chemical weapons)

Although the above may appear being unrelated, it is possible that sensors outputs from different sources and areas could in fact be part of the same scenario. It is therefore necessary to be able to understand and evaluate all sensor outputs under a common reference. Besides, in order to achieve holistic overview of the area being monitored, we should not examine each sensor's operation individually but also with respect to the sum of inputs received. Data are planned in being fused in C2 operations, so as to deliver logic interrelations and additional insights upon the situations detected.

3.2 Key functionalities in Situational Awareness

3.2.1 Network Requirements

3.2.1.1 *Network Complexity Requirements*

Public Safety end users require that network availability is provided at all times, due to the crucial nature of the data and circumstances being handled; even a few minutes of delay or malfunction in the network, could result in security threats of significant magnitude. For that reason, Public Safety organizations often prefer private network providers who can guarantee more than 97% availability at all times. This attribute is further explored in Section 4 – Ad Hoc Networks.

Public Safety end users also require that the network of sensors in the field may be scalable and flexible, able to host an infinite number of nodes, taking under consideration that we are looking into providing a complete city-wide security support. In fact, one of the main characteristics of the platform in a large-scale surveillance system is **heterogeneity**. End users come to utilize a set of different families of sensors, being differentiated upon a) areas of operation (e.g. CCTV camera, environmental sensors, etc), b) types (e.g. thermal cameras, etc), c) data types and formats, d) manufacturers and providers. It is also important to provide efficient solutions for different scenarios ,especially when scenarios refer to cases of emergency.

Ultimately, serious concerns regarding the effective management of the network traffic, storage and performance become apparent. First of all, the integration of a set of heterogeneous devices raises complex security concerns, requiring dedicated security layers to cope with e.g. authentication process (for allowing a sensor device to connect to the network), different encryption specifications upon the output data, etc .Additionally, the main sensor outputs being delivered across a Public Safety network include video data streams, transmitted as live or stored video outputs. In both cases, the bandwidth requirements are high, while as technology progresses and new camera sensor can provide higher quality, end users expect that the network providers will be able to follow these demands.

The management of a grand set of heterogeneous signals needs to be realized prior to the data reaching the C2 center level, or else we could risk experiencing data overload, increased latency, data loss or even information loss, i.e. sensor outputs failing to be appropriately processed due to increased traffic, causing missed detections. End Users seek to enable acquired data suspended to some basic pre-processing, prior to reaching to the C2 centre.

Temporary database storage of the sensor outputs is necessary for the effective network operation. Stakeholders' requirements typically range within 20-40 TB[1], assuming a 7-days storage interval[2]. However, flexible and scalable data storage needs to be enabled so as to cope with changes in the network operation (e.g. including a new sensor in the network).

Finally, data transmission also needs to be realized at low latency, in order to enable near-real-time operation.

3.2.1.2 *Sensor networks and their requirements*

The networking infrastructure will comprise of many different network types, which of course all those have to be interoperable, but the most novel aspects of the information handling in that environment can be found in the **wireless sensor network** part. Further to the network requirements described above, we estimate that SafeCity sensor networks require:

- the ability to **adapt** to a changing environment, and in particular changes in topology, availability of resources and data volume
- to be scalable, and accommodate the thousands of devices that are scattered throughout a city
- the ability to handle a sudden surge in network traffic when an accident or crisis occurs
- to minimize redundancy of information so as to notify in an effective manner all appropriate authorities and emergency response teams
- to rely on power-aware protocols as nodes rely on batteries whose replacement is often impossible or impractical
- to provide local composition of data, **data aggregation** and error correction to assist in turning data into useful information
- to ensure that data collected by the sensor nodes may not immediately transferred to the central system to increase the robustness of the system and to reduce communication needs. Thus not all traffic is necessarily synchronous. For example, there may be a need to support direct voice or video communications but, equally, delay tolerant traffic may be of significant value. Assume, for example, a CCTV camera equipped with a wireless interface uploading a static image to a support vehicle that downloads that to the surviving fixed infrastructure the next time it passes any. It may take minutes for the picture to reach a control centre, but this is

[1] Further technical details upon the end users requirements can be found in SafeCity deliverable D3.1 – Specific Requirements Definition

[2] Based on legal regulations upon the temporary storage of sensitive data

still information of significant value, especially compared to sending in a human observer to obtain the same information

- to adapt their processing capabilities in response to external control through the middleware they contain. This may necessitate a **discovery** service in order to locate the appropriate components, since we cannot assume that every device is pre-loaded with components implementing all such protocols

3.2.2 Data Management

The most important aspect of data management in Safe City is of course security. The data security is assured by the functionalities described in Privacy &Access and Communicational security below, but data management includes data interoperability, filtering and meta-data functionalities to assist data security.

3.2.2.1 Data interoperability and filtering

Safe City Data is provided from different sources. Each of them, provide as many information as is available. The problem arises when that data should be understandable by command centers. This means understand the data and gather as many structured information as disposable: when, where, how, who and what. Having a data interoperability enabler will make data transparent from specific representation, but available for all those artifacts wanted to use it.

Data filtering is also extremely necessary. Huge amount of data is generated at a given point on time on several locations all over the city. Regular data has no more value than “everything is ok”. For instance, regarding regular weather conditions, temperature and traffic flow.

In some exceptional cases, the ones important for the SafeCity context, data become critical, and some kind of safety critical system should deal with all data. For instance, when an Emergency Declaration is broadcasted due to a fire in the city center, priority should be focused on analyzing the data associated to the location of emergency, setting as secondary the rest of data produced by the system.

3.2.2.2 Metadata

One key requirement raised under this consideration is the ability to introduce standardization of the input video streams. It is difficult to force a standardization model, as opposed to introducing a pool of semantics as key reference in the description and interpretation of all inputs being handled. This in fact should be a definition of semantics to be applied commonly in all Public Safety Use Cases, thereby including the entire set of basic PS ontology required. The SafeCity project is going to conceptually explore and define the design of the SafeCity Ontology, in later research[3].

Besides, PS stakeholders require that the sensor outputs reaching the C2 processing facilities and infrastructures carry basic meta-data information, including timestamp and location, or even basic tags upon the main attributes of the acquired image (e.g. in the cases of traffic violations, meta-data should include plate recognition, speed, motorway-associated with location, etc). While timestamp and location information metadata may be delivered from the network (e.g. with the usage of NTP servers), the SafeCity Ontology could be specifically delivered to Public Safety Use Cases, and cope with more specific requirements and needs.

Apart from the standardization of output sensors, Semantics it makes possible to provide a set functionalities such as: semantic searches (showing not only the matching elements, but also the related ones), reasoning engine in order to infer new knowledge from previous stored one, manual annotation in order to introduce expert knowledge in a easy way and ease the possible shortcomings of Learning

[3] SafeCity deliverable D3.2 – Global SafeCity Framework Characterization

algorithms. Finally, the introduction and referencing of PS ontologies would enable different PS organizations' inputs to be merged easily and automatically. This description is further detailed in section 5.

3.2.3 Surveillance Capabilities

The main operation related to Situational Awareness is the ability to monitor an area and identify threats in it. Currently, most of the PS organizations acquiring video inputs typically rely on human operators to detect abnormalities and suspicious behaviors. This implementation is inefficient both in terms of resource and accuracy:

Resources:

- Infrastructures: necessity to include wide screens for effective visualization of sensor inputs
- Working staff: dedicated positions in observing the set of images acquired by sensors

Accuracy:

- Grand amount of inputs: resulting in the need to monitor a set of cameras per operator, that set being beyond the observing capabilities of the officer in charge→ possibility of missing elements
- Human factors: misjudgment on the identification of suspicious or not images

PS end users require that most of the video data processing would be realized automatically, requesting only minimum to none human intervention. In particular, automatic detection (video analytics) on pre-defined patterns, a priori known as being suspicious, would ease work operations in C2 centers and speed the decision making and response phase.

In continuation to the above point, efficiency of data processing techniques would be better achieved if the indicated alerts were produced in the early stages of abnormalities expression, thereby enabling not only the recognition of a pre-defined pattern of suspicious elements, but also its prediction, using Intelligent video analytics algorithms and simulators.

However, at the same time, PS end users are concerned with the level of false alarms activated during operations[4]. As mentioned above, this is a risk possible to occur even under the close surveillance of human operators, however most often false alarms are triggered as consequences of malfunctions in automated processes. Sources of mistakes could for example include the non-universal adaptability of processing algorithms, i.e. defining threshold values of certain indicators triggering alarms, and such indicators being away from the pre-defined range in certain areas and/ or scenarios. Such inconsistencies are usually difficult to detect and basically conquered by experience on the field, but could be controlled with additional levels of processing and cross-referencing procedures, and self-learning designs.

It is worth noting however that Artificial Intelligence Algorithms are worst in terms of accuracy than a trained operator (for one image). Supervised Learning Algorithms suffer from over-adaptation/over-fitting making it difficult to generalize to other sets different of the training set. Additionally is very difficult define all the possible suspicious behavior for a PS, therefore collaboration between machines and humans are essential.

In spite of the fact that humans (trained operator) have more accuracy to detect suspicious behavior than a machine learning algorithm, the number of images that a human operator can analyze in a parallel way are roughly 3 o 4, whereas a computer are practically unlimited. Therefore the computers

[4] Reaching up to 20% in Traffic Surveillance

should assist to humans, selecting the most suspicious behavior and showing it to a human operator, finally the decision are going to taken by a human operator.

Automatic detection (video analytics) on pre-defined patterns, requires a priori knowledge about suspicious behaviors, however this knowledge resides in the operator. Therefore could be interesting provide a set of functionalities (like manual annotations) in order to insert this expert knowledge in an easy way. This approach would ease work operations in C2 centers and speed the decision making and response phase.

Looking now in particular each of the surveillance areas defined in Situational Awareness, we present the following requested functionalities **(Tables 3-6)**:

Suspicious citizen behaviors criteria typically place attention on:	**Which can be intelligently modeled by:**
Public concentrations and riots	Tools for counting person concentration
Expressions of aggressive behavior and criminal activity (e.g. theft)	Detection of motions and patterns assessment
Serial thefts	Identification of similar patterns and intelligent deduction of next move predictions
(location) Critical places	Awareness upon security exits, hospitals, train stations, etc
(time) Time of day	Awareness of expected behavioral routines per time of the day, identification of deviations in terms of time intervals
(behavior) Deviation from “normal activity”	Modeling patterns based on the above (location and times) in progress

Table 3 Functional requirements related with the detection of suspicious citizen behaviors

Suspicious objects criteria typically place attention on:	**Which can be intelligently modeled by:**
Abandoned objects	Recognizing human activity near the object over the past time intervals
Movement of items in high risks areas	Definition of kind and size of object
Shape characteristics	Awareness on typically expected sizes and deviations

Table 4 Functional requirements related with suspicious objects’ surveillance

Suspicious vehicles criteria typically place attention on:	**Which can be intelligently modeled by:**
Stolen cars	Car features detection
Irregular parking	Time, access zones, etc
Traffic congestion and congestion loads	Keeping records of peak times & zones Distinguishing levels of traffic flow based on its speed and zone occupation

Traffic incidents	Identification of car accidents, automobiles failure, etc
Restricted vehicle behavior	Detecting cars crossing to opposite lanes, stopping in forbidden areas, etc
Environmental conditions disturbing traffic	Awareness and effect of heavy weather conditions in the area
Road Safety	Road condition detection, identification of problems in constructions, disturbing objects, etc

Table 5 Functional requirements related with suspicious vehicles' and traffic anomalies' surveillance

Environmental surveillance criteria typically place attention on:	**Which can be intelligently modeled by:**
Malicious air substances	Specific molecular concentration detection
Malicious organic footprints	Analysis of thermal radiation with respect to expected radiance patterns (per area, per time of the year, etc)
Alarming environmental indicators	Increased surface temperature and/or gas consistency, alerting the outbreak of fire

Table 6 Functional requirements related with suspicious environmental indicators' surveillance

3.2.4 Privacy & Access Control

While real time detection of threatening patterns is required and while data being pre-processed and meta-data enriched when reaching the C2 infrastructures, the sensor network on the field cannot have direct access with the C2 databases. For example, mobile Police units may detect suspicious behavior of a driver on the road. The protocol states that the plate information of the vehicle shall be transmitted to the C2 centre, where via internal and secure network infrastructures it shall be compared and retrieved from the organization's databases. Finally, a feedback shall be sent to the mobile unit.

The above configuration is a very important aspect in PS organizations: criminal databases cannot be accessed via public networks and need to be stored and accessed via private and secure infrastructures. Of course accessing such databases, even within the organization's private network needs to follow secure protocols (user password and authentication), while concrete logs of the activities realized need to be maintained (auditable databases).

Additionally, access in these databases should present varying levels of security and encryption definitions, depending on a) the type of data being retrieved and b) the user who tries to retrieve them.

While the entire set up of the databases should be considered in Section 5 – C2 centers, the current section tries to determine the methods for accessing stored information and information allowed to be transmitted, via enabling dynamic set up of security levels.

3.2.5 Communication Security

Finally, one of the major concerns is that of **security**. The ability to distribute arbitrary code to nodes that are not normally under the direct control of emergency authorities is a sensitive issue, as is the ability to arbitrarily collect data from sensor nodes and to control the actuators that one normally regards as being personal. Another very important issue is to manage the trade-off between the level of security and the efficient use of resources and in parallel to enable a scalable security framework for various applications. To be able to add nodes to the system there must be some kind of key management processes. These processes will involve human interaction, especially when introducing new nodes. Directly related to this there must also be some ability to delegate rights to nodes and to generate cryptographic keys in a centralised or a decentralised way as also to enable energy savings and a corresponding set of light-weight security.

In traditional distributed security, authentication is established after contacting a trusted authority responsible for maintaining up-to-date record of each user's access rights. However, in a disaster response scenario, communication with this authority might be poor or even impossible. In such a case a best-effort security model may be more appropriate. Approaches based on public key cryptography overcome the need for a trusted authority but the computational requirements are high considering the resources available on sensor nodes. Algorithms implementing elliptic curve cryptography are believed to be more computationally efficient than the former.

3.2.6 Additional requirements-Ethical Constrains

Ethical considerations exist in ICT and Surveillance operations and in fact PS organizations need to follow EU and nation-wide regulations, so as to ensure that their application do not jeopardize the well-being of citizens, by trespassing rights upon citizen privacy, equality, etc. While most of the considerations regarded[5] are more closely related to strategies and protocols being adapted by the PS organizations, many restrictions may in fact be enabled via technical developments. In this way, developers and providers assure up to a level that their services are transparent with regard to existing policies and regulations.

First of all, regulations exist to control the temporal storage of sensitive data, typically varying around seven (7) days, as mentioned above in the network storage capacity requirements. Secondly, the definition of abnormal and suspicious behaviors should be not be based on social, religious, racial, etc discriminations, but rather on subjective indications of criminal patterns, as it was presented above in the Surveillance criteria.

Strict security mechanisms need to be applied for the protection of recorded images, once these are being specified as sensitive data. Such mechanisms should involve rules and monitoring upon the data retention, disclosure and disposal and monitoring. Variations in nation-wide regulations permit different types of sensor sources to be incorporated, for example Greek law only allows the installation of traffic monitoring in high-traffic roads. Security mechanisms based on metadata annotations regarding the sensor information could provide a filter of the information which should be stored, processed and disposed or not.

Finally, in order to ensure that surveillance operations do not violate the citizens' right to privacy, PS end users require that the network of the deployed sensors must not acquire images from private site. This could be a difficult specification, if we consider for example the case of a house being sited near a central city square. However, intelligent software applications could be used to provide masking functionalities, when the sensors exit public view.

[5] SafeCity deliverables D7.1 – Social, Ethical and Legal Implications, D7.2 – SafeCity Policy Making

3.3 Summary of Operational Requirements

In summary, the following sets of key requirements are found necessary in the Public Safety Situational Awareness systems:

3.3.1 Network

The network requirements are very demanding, arising from

- The communication infrastructure – This must support both the local, mobile, wireless and the fixed wire-line stationary network connections. It **should be able to make use of whatever communications systems are available in a particular environment**
- The nature of data being transmitted (multimedia) – **High Bandwidth**
- The rate of transmission (ultimately leading to huge data storage needs) – **Big Data Storage**
- The need to provide near-real-time surveillance – **Low Latency**
- The ability to extend and host multiple sensors – **Intelligent Management and QoS, Bandwidth management**
- The ability to remain operating even under crisis situations with the **introduction of ad hoc and mobile networks to resume communications**
- The need to ensure data integrity and avoid data loss – **Security and Trust mechanisms**

3.3.2 Data Management

C2 centers operation would be favored by the referencing of inputs under common formats:

- **Data interoperability** and **filtering** is needed
- Inputs **standardization** and databases **integration**
- Data need to be enriched with **timestamp and location information**
- Data need to be **enriched with basic attributes** regarding the detected incident
- **Different interfaces** will be required for all categories of information; Starting from high priority directives, **high priority sensed data** should be **mixed** with informational and general reporting data
- Definition of **SafeCity ontology** to use a reference in PS applications, data tagging enablement at sensor level

3.3.3 Surveillance capabilities

Applications should be defined to intelligently detect suspicious patterns

- Surveillance of suspicious objects, citizens and vehicles – Video analytics to analyze images based upon criteria (patterns, time, location, repeats, etc), realize object **tracking**, facial **recognition**, **prediction of behaviors**, etc
- **Automatic detection of threats** – Video analytics to detect given and pre-defined patterns in the images
- **Intelligent surveillance requiring minimum human intervention** – Cross referencing of detected patterns and self-learning capabilities to deal with false alarms

3.3.4 Privacy, Communication Security and Trust

Sensitive data need to be security protected against unauthorized access and usage:

- Databases need to be maintained in private premises and only be accessed via private networks – **Private cloud infrastructures**
- Databases need to be secure and auditable – **Security, trust and authentication mechanisms**
- Databases need to have dynamic and variable encryption level based upon data being stored and data aimed to be transmitted –Rules and mechanisms for **dynamic setup of security databases**

- Important information must be segregated, reported properly and in a sensitive manner for the audience at the right level – Appropriate personal data management policies and **standarized formats to respect and protect** their **sensitive content**

3.3.5 Additional concerns

Citizens' privacy rights need to be respected, as follows

- Sensitive data need to be protected against their storage, processing, distribution, etc processes – **Security mechanisms for personal data management**
- Private places need to be assured not to be monitored – **Intelligent software masking functionalities**
- Data sources and types need to comply with nation-wide regulations – **Security mechanisms based upon metadata annotations to filter incoming data**
- Reporting to authorities and central systems should occur in accordance with the privacy and security provisions mandated by EU directives – **Additional Policy Making and Ethical/ Legal Management required**

3.4 Generic enablers to support the Situational Awareness Operations

Following, we present the Core Platform capabilities that we initially take under consideration in order to deliver the operational requirements posed by the PS end users, as described above. **Table 7** below presents those generic enablers found delivering part or most of the required functionalities. A brief reference of how these enablers are found functionally needed is presented in [2], while future updates of the current document are also expected to deliver more low-level details. Functionalities not delivered by those definitions are explored in the description of new enablers in Section 3.5.

FIWARE reference	Name
3.2.1	IaaS DataCenter Resource Management
3.2.2	IaaS Service Management
3.2.3	PaaS Management
3.2.4	Object Storage
3.2.5	Cloud Edge
3.2.6	Monitoring
3.2.7	Resource Metering and Accounting
4.2.1	Big Data Processing
4.2.1	Publish/Subscribe Broker
4.2.2	Complex Event Processing
4.2.3	Multimedia analysis to gather multimedia meta-data
4.2.3	Big Data Analysis
4.2.4	Multimedia analysis
4.2.4	Pre-processing of meta-data during/after gathering
4.2.5	Preprocessing of unstructured data
4.2.6	Meta-data Pre-processing
4.2.6	Localization Platform
4.2.7	Query-access
4.2.8	Publish/Subscribe Broker
4.2.9	Semantic Annotation enabler
4.2.10	Semantic Application Support enabler
4.3.1	Social Network Analysis
4.3.2	Mobility Analysis
5.2.2	USDL Service Descriptions
5.2.3	Model Repository
5.2.8	SLA Management

5.3.3	Composition editor
5.3.4	Application mashup editor
5.3.5	Service composition
5.3.6	Execution engine
5.3.7	Mashup execution engine
5.3.8	Service composition engine
5.3.9	Service orchestration engine
5.3.10	Aggregator repository
5.4.1	Data Mediation
5.4.2	Protocol Mediation
5.4.3	Process Mediation
5.5.1	Multi-channel/Multi-device Access System
6.2.1	IoT Communications
6.2.2	IoT Resources Management
6.2.3	IoT Data handling
6.2.4	IoT Process Automation
7.2.1	Connected Devices Interfacing (CDI)
7.2.2	Cloud Edge
7.2.3	Network Information and Control (NetIC)
7.2.4	Service, Capability, Connectivity, and Control (S3C)
7.3.1	Identity and privacy management
8.2.1	Security monitoring
8.2.2	Identity Management
8.2.3	PrimeLife Policy Language (PPL) Engine
8.2.4	Identity Mixer (IdeMix)
8.2.5	Context-based security and compliance
8.2.6	Optional Security Service Enabler

Table 7 Core Platform Enablers requested for the delivery of the SA requirements

3.5 Situational Awareness Specific Enablers

3.5.1 Network Enablers

3.5.1.1 *Semantic Gateway*

Related Functionality

<u>Handling heterogeneous sensors, filtering data upon severity and managing traffic upon sensor inputs and UC priorities</u>

Description

The Semantic Gateway enabler will be operational in conjunction with the Semantics Definition of Suspicious Patterns enabler and data pre-processing techniques. The idea is to allow intelligent network traffic control based upon the surveillance requirements of the network. Under this context, the Semantic Gateway enabler will deliver data routing and QoS, acting like a regular gateway installation, yet it will do so by applying priorities rules acquired from the semantics of the data acquired. The overall operation is expected to deliver better network control and preparedness at the C2 centre.

In this sense, the overall process may be described as follows:

- Data are being acquired from the sensor network and are being temporarily stored on a gateway server (e.g. FIWARE Cloud Proxy GE)
- Data are being subject to local processing techniques, holding partial capabilities as the ones taking place in the C2 center (e.g. FIWARE Pre-Processing of unstructured data GE)
- Based upon the processing result, data are becoming enriched with metadata information related to the C2 criteria (e.g. SafeCity Ontology, FIWARE Semantic Annotation GE)

The above are necessary processes to be realized in order to allow the operation of the Semantic Gateway enabler which will be in charge of:

- Evaluating the importance of the data being transferred based upon their semantics annotations (e.g. detected threat vs. none, types of threat, etc)
- Realizing intelligent data fusion upon data holding similar semantics upon the event detected, location and timestamp
- Arranging data packets based on the above considerations, setting network priorities to match the sensor inputs

Features/ Supported Functionalities

The enabler is going to be composed of the following components, each delivering a respective functionality as presented below:

Component	Functionality
Ontology Prioritization	This feature will make use of the available and pre-defined semantics and shall arrange the priorities of the ontologies given. Initially this will be designed de-facto to serve user needs and being oriented upon generic PS definitions. Upon operation, the feature will be able to self-update either manually based on the user's considerations, or automatically by detecting the behavior and characteristics of the given network, miming abilities of a reasoned engine
Semantic-based Data Fusion	This feature will provide data mining upon the criteria set by the Ontology Prioritization feature. Additional attributes will include location in 3D (altitude, longitude, latitude), type of sensors, timestamp, etc

Data Routing	The final feature will deliver the basic gateway operation based on the semantic criteria and data fusion techniques defined above. At this stage, the data routing component will assemble data in the forms of packages with according traffic priorities and forward them to the main network

3.5.1.2 *Service availability estimation*

Related Functionality

Bandwidth estimation, QoS support and resource management

Description

Mobile actors will benefit from predictions of available services at present location and time, including estimations how the service availability will change. In particular, early warning about communication disruptions will guide mobile actors on what can be expected in terms of cloud applications/services. The need for this is due to the dependence of wireless communications, or wireless networks for mobile actors. Furthermore, the service availability varies as a frequency of the changing network conditions, due to the difficult propagation conditions at some location, limited bandwidth resulting in overload etc.

Features/ Supported Functionalities

The enabler is going to be composed of the following components, each delivering a respective functionality as presented below:

Component	Functionality
Availability Estimation	The component will estimate the present communication link status and predict the future status of links to mobile users. In cases of several links to a mobile user, all links will be treated under the coordination of a produced jointed availability estimation
Link quality estimations	The component will measure the quality of the links (e.g. considering Signal-to-Noise-Ratio, etc) being in use. In case existing communication links are of low quality, other possible radio interfaces at the platform/user will be activated and their links will be investigated
Traffic estimation	The bandwidth/traffic needs are estimated and these needs are compared to the available bandwidths obtained through the link estimation. As long as enough bandwidth for the traffic is available, no further steps should be required. Otherwise, future traffic demands are estimated, along with predictions upon the changes to take place in the link qualities (e.g. using a propagation path loss model based on distances and how the user move)
Presentation & security	The component will for a given user when the service is requested produce a report showing present joint link status and an early warning in case deterioration of service availability and disruptions is likely in the near future. Moreover, authentication will be required in order to securely activate the service

3.5.2 Data Management Enablers

3.5.2.1 *Semantic Definitions of Suspicious Patterns*

Related Functionality

Handling of heterogeneous information and sources, delivering abilities for advanced C2 control operations (search, relate, etc)

Description

The enabler looks into the importance of semantics in Public Safety applications. Indeed, the integration of such an amalgam of different sensor types, manufacturers, etc raises necessities upon a standardization process to be obtained. Additionally, as described in the network enablers, a general semantic pool defined across the Public Safety operation network would allow more effective traffic and sensor control. The Semantic Definitions of Suspicious Patterns enabler is expected to be a dynamic ontology collection of PS semantics and priorities as reference both in processing modules (e.g. search for a given semantic annotation in the input acquired), but also in network configurations or even in dynamic security settings over the data being transmitted.

Features/ Supported Functionalities

The enabler is going to be composed of the following components, each delivering a respective functionality as presented below:

Component	Functionality
Threat Ontology Definition	This component is going to introduce definition of suspicious behaviors/patterns list and association with visually perceived events/objects in video data and rules with respect to their dependency and inference of higher levels on knowledge (semantics)
Metadata generation	This component is going to introduce the ability to generate low (visual descriptors) and high level (semantic) metadata with findings that will be machine processable by other applications or by human operators, assisting the visual presentation of the identification results. Stored in the database and associated with the original raw video data
Reasoning Engine	This component is going to introduce the ability to use inference algorithms (e.g. description logics or FOL) and properly defined domain ontologies and rules based on spatial-temporal relationships of detected objects/events in visual data in order to infer higher level semantics. This is concerned mainly on how to assess the spatiotemporal sequence of a variety of detected objects and events into a semantically defined suspicious behavior instance (i.e. characterize wandering).

3.5.3 Surveillance Capabilities Enablers

3.5.3.1 Suspicious Objects Detection

Related Functionality

Automatic detection of threats concerned with orphan objects, contained weapons, etc

Description

The enabler offers the ability to define suspicious objects based upon their relation to their background. This may refers to

- Noticing that the object remains orphan (i.e. unattended) for a significant time
- Noticing that the object presents suspicious size and/or shape
- Noticing that the object does not appear to belong in the background

Features/ Supported Functionalities

The enabler is going to be composed of the following components, each delivering a respective functionality as presented below:

Component	**Functionality**
Under-object inspection	This looks into the content of suspicious objects. The component should allow detection of explosives, weapons, drugs, chemicals, etc based upon texture analysis and shape recognition. The component will act upon a) a layer of definitions regarding where to search for suspicious objects – e.g. a back bag, and b) the patterns and descriptions of the suspicious objects to be searched for
Orphan object detection	The component will deliver the ability to analyze the motion patterns of moving objects looking for discontinuity in motion patterns for a significant duration.
Moving Object Segmentation	The component will deliver the ability to process and analyze motion and other visually perceived characteristics of the video data (color, texture, shape, temporal continuity, etc.) in order to segment motion data and detect moving objects

3.5.3.2 *Suspicious Citizen Behavior Detection*

Related Functionality

Automatic detection and prediction of threats concerned with suspicious citizens

Description

The enabler will make use of pre-defined semantics and definitions of abnormalities in order to detect normal vs. suspicious behavior. The second are further being considered in terms of more specific activities and scenarios and so, according features have been defined to introduce the respective processing capabilities.

Features/ Supported Functionalities

The enabler is going to be composed of the following components, each delivering a respective functionality as presented below:

Component	Functionality
Detection of suspicious motion	The component will make use of intelligent algorithms interpreting motion patterns in order to identify based on basic body gestures, underlying criminal activity and/or intention. The outputs may be quite abstract, i.e. delivering only a possibility of alarm, so further attention should be required by the controller. Additionally, the component will deliver insights on suspicious motion and/or loitering patterns, defined with respect to background information, e.g. a person being close to an ATM machine for a long time without using it. This would also be expanded to include detection of vandalism activities. For the second case of operation, additional inputs regarding critical places of increased interest should be able to be entered by the user.
Active Learning	The component will include a cluster of intelligent agents acquiring feedback upon the alarms detected and/or missed. Also, the aim is to allow the enabler to self-develop and adapt to different circumstances by detecting more high-level characteristic similarities. Self-learning properties will be enabled to allow the overall behavior of the enabler to become intelligent, requiring minimum human interventions.

3.5.3.3 Detection of Violation to Restricted Areas

Related Functionality

Automatic detection and prediction of threats concerned with unauthorized access

Description

The enabler is going to provide support for cases where unauthorized access in secure premises is realized. This has several applications in critical buildings and sites, such as airports, stations, banks, etc, while it may also find use in areas of low visiting frequency, e.g. restricted industrial/ military premises, etc. The importance of the functionalities delivered lies on the fact that there needs to exist a distinct separation between

- The areas which do not need to be protected, implying that for example in the case of an airport, citizens need to be able to navigate through the public places freely without feeling burdened by the security measures on the background
- The level of security required in each restricted area, meaning that some sites may be exclude any time of intrusion, while other may allow access to given parties (e.g. authorities, controllers, etc); for that reason, the enabler may also be found working in parallel with the Face Detection & Identification enabler, so as to distinguish between false alarms

Features/ Supported Functionalities

The enabler is going to be composed of the following components, each delivering a respective functionality as presented below:

Component	**Functionality**
Trespassing detection	The component will directly deliver the ability to detect a person/object passing within the area defined as restricted. In order to realize that, the component will make use of applications for Virtual Line Drawing, enabling the marking of several lines surrounding an area, in order to use them as reference for “borders”. When a trespassing is detected, i.e. a virtual line drawn has been interrupted by a person/object, the component will trigger an alert to be evaluated by a) the False Alarms Handler and b) the Access level control, if applicable
Motion detection	This feature will emerge from video processing applications, making use of intelligent motion estimation/detection algorithms. The feature may be proven highly valuable in cases where such an intrusion has been accomplished that the Trespassing detection has not been able to detect it (e.g. underground access) and/or where the user needs to be aware of the motion within an area (i.e. the user is aware of motion activity in the restricted area, but needs to maintain it restricted and controlled)
Background differences analysis	This component will deliver the ability to detect differences in the background by comparing two distinct input values, most likely a current value being studied and a past value having been specified (and verified) as either a a) highly secure point (looking for differences), or a b) dangerous point (looking for similarities). The second input image shall be used as reference. The component should be able to analyze multiple formats of multimedia input
Access level control	As mentioned above, it might be the case where an area needs to be restricted, yet certain authorities should be able to access it (e.g. secure premises in an airport). The component will mainly act as a controller of behavior for the enabler, marking its detected alerts as true or false. Many facilities have an access level control mechanism installed at the entrance of such areas; in this case, the component should be able to link and verify the access granted, so as to characterize the

	detected motion as “safe”, i.e. do not generate an alarm. Alternatively, the component could be used in terms of directly receiving user criteria for facial exceptions. In this case, the enabler will be linked to the Detection and Identification enabler, so as to make use of the facial definition capabilities
False Alarms Handler	Many often, high security measures like the case described suffer false alarms being caused by detected motion which is however unharmed, e.g. an object falling due to an earthquake/ wind would enable the detection of motion activity, but would not be an alarm, additionally a domestic animal accessing a restricted open area would not be an alarm. The False Alarms Handler component will be aware of all detected intrusions, including a) their patterns and b) the respective component which triggered them. The component will compare the detected signals against a dynamic database, based on self-learning capabilities, holding both “dangerous” and “excluded” patterns. Finally, regardless of the final marking of the alarm (true or false) the component will try and identify the location (within the image) of the detection and its perceived category of intrusion

3.5.3.4 *Detection & Identification*

Related Functionality

Specific features recognition (citizens and objects), identification of specific patterns across a crowd

Description

The Detection & Identification enabler is going to provide the ability to detect a given pattern (facial and also object) among crowds, using a two-directional process:

- The enabler may search for a set of specific characteristics in the crowd/ environment, upon request after being fed a specific information from the C2 database; related scenario includes e.g. the active search of prisoner who escaped
- The enabler may define given characteristics in the crowd/ environment, i.e. detect a suspicious pattern, scan characteristics and upload them for comparison to the database; related scenario includes e.g. the detection of criminal activity and the real-time procedure of identifying the suspect

We should note at this point however that such detection and identification techniques may be found being against national laws concerning personal data security. For that reason, it is necessary to validate the legal and ethical framework upon which the Detection & Identification enabler is expected to operate upon.

Features/ Supported Functionalities

The enabler is going to be composed of the following components, each delivering a respective functionality as presented below:

Component	**Functionality**
Visual facial descriptors extraction (offline)	Video processing to extract visual facial descriptors (color, shape, size, symmetry, etc.) producing low-level visual metadata, invariant to scale and color variations (as lighting may differentiate during day and night). Such meta-data should be enriched in order to allow identification even upon disguises.
Face detection	The component will deliver the ability to detect a face in a video stream or captured video/image, by making use of color and shape information. The outputs should be spatial/spatial-temporal (if tracked) face regions, which can then be used further to apply face recognition.
Face recognition	The component will deliver the ability to compare a captured image/video of a face in frontal view, and its visual facial descriptors to another stored face model of the same descriptors for faces of persons existent in the database, and identify that one that corresponds to the same person as the person in query, even if the models are not identical (in fact they are typically quite different).
Object recognition	The component will deliver the ability to recognize a given object pattern defined as suspicious, based on texture, shape, size, etc analysis.

3.5.3.5 *Real-time Positioning and Tracking*

Related Functionality

Position awareness and tracking capabilities upon given patterns, across neighborhood sensors

Description

The Real-Time Positioning and Tracking enabler is going to deliver 3D representations of suspicious citizens upon 3D images of the area monitored. The enabler is going to incorporate input from the installed CCTV network in the area and also abstract information from intelligent algorithms when such information is not available. The enabler is going to deliver as main functionalities the following:

- Calibrating sensor inputs, acquired from an amalgam of different camera images
- Predicting behaviors, such as individuals paths and/or crowd movements based on model knowledge and analysis
- Tracking pointed persons

Features/ Supported Functionalities

The enabler is going to be composed of the following components, each delivering a respective functionality as presented below:

Component	**Functionality**
Person and moving object tracking	The component will provide the trajectory of one or more persons across different sensors in an area. The procedure will be based on spatial coordinates/timestamp information, i.e. spatial-temporal trajectory in the video data and it is also going to be supported by GPS tracking. Additionally, the component will allow tracking over time detected moving objects based e.g. on temporal continuity of its motion and spatial features. Both these capabilities can be used in combination with Suspicious Object and Suspicious Citizen Behavior Detection enablers. Also, the feature will require access to controlling sensor capabilities (see C2-Video Analytics enabler).
Video synchronization	This feature will allow the synchronization of the video inputs being received. This is necessary in order to work upon a unique time reference, so as to enable correct tracking and behavior modeling. The feature will require external support from network specifications in order to enrich data with timestamp metadata and/or the implementation of an NTP server.
Behavior Prediction	This component is going to include intelligent agents and artificial intelligence for recognizing patterns and define predictions in behaviors and crowd assemblies upon model-based knowledge. Clearly this feature will be able to recognize basic behavioral patterns and to analyze them across spatial and temporal variations, as well as basic environmental attributes

3.5.3.6 Traffic Violation Detection

Related Functionality

Automatic detection of threats related to traffic behavior

Description

The enabler will be able to deliver the following functionalities and characteristics:

- License plate detection and storage if any vehicle jumps signals (red light violation detection).
- Detection of a car in a wrong way road.

Once a violation is detected, the Real-time Positioning and Tracking enabler could be used to track the respective car, based on the acquired details upon its characteristics.

Features/ Supported Functionalities

The enabler is going to be composed of the following components, each delivering a respective functionality as presented below:

Component	Functionality
Wrong Lane Violation	The component will include capabilities for detecting wrong driving behaviors regarding the lane the car is expected to be on. This includes the possibility of a driver passing in the opposite lane (e.g. for passing another car, not being to control the wheel, etc) but also when some lanes have been defined as temporarily out of service (e.g. in the case of an accident, routine maintenance, etc). For the component to work, it is necessary to be connected to the on-the-road sensors, and also the criteria of each area. For example, across which areas is it forbidden to overpass? Also, in order to care for routine emergency restrictions, the component should be able to acquire manual and/or automatic updates on the respective cases to be looked for.
Traffic Light Violation	The component will also be connected with on-the-road sensors detecting a) whether a car has crosses a red light, b) what was its speed when crossing, c) what was its speed a few meters back and d) the weather conditions in the area. The aim is to separate among the cases where such a behavior should be marked as violation or whether it falls under the cases where the driver would have cause more serious damage if he would have stopped.
Speed Limit Violation	This is also going to acquire data from installed sensors on the road measuring the speed of the passing cars. Speed limits change across areas and also with respect to a) weather conditions, b) accidents in the area, c) increased traffic, d) maintenance, etc. In this sense, the according updates also need to be fed into the component for evaluation of the violations detected.

3.5.3.7 Environmental incident detection

Related Functionality

Automatic detection and prediction of threats triggered by environmental indicators (fire, bio-chemical attacks, etc)

Description

The enabler will be able to deliver the following functionalities and characteristics:

- Early detection of fire, gas, smoke
- Early detection of high level of contamination

Features/ Supported Functionalities

The enabler is going to be composed of the following components, each delivering a respective functionality as presented below:

Component	Functionality
Fire Detection	The component will acquire input from an amalgam of sources including thermal cameras, smoke detectors, temperature controllers, etc and will use combination algorithms to evaluate potential abnormalities. The component should make use of different spatial and temporal features when in operation, and it should also include a wide range of according threshold values to be compared against
Contamination Detection	The component will also make use of a wide spectrum of sensors, including thermal cameras but mainly environmental sensors searching for key indicators. The component should allow an active learning and dynamic adaptability to changing bio-chemical threats

3.5.3.8 *Cold vehicles*

Related functionality

Definition of risk of cold vehicles in a traffic jam on a certain road section using information from temperature, infra-red and video sensors as well as statistical prediction models

Description

The enabler will estimate the need for evacuation of people from cold vehicles in traffic jams under cold winter conditions. After a time in a traffic jam, there is a high risk of vehicles running out of fuel so that people cannot keep warm any more. In such cases, old people and children must be evacuated from the road and also vehicles have to be removed from the road.

Features/ Supported Functionalities

The enabler is going to be composed of the following components, each delivering a respective functionality as presented below:

Component	Functionality
Cold vehicles evacuation report	The component will provide a report including an estimation of the number of vehicles on a road segment, expected to run out of fuel and that need to be evacuated
Decision support	The component should be activated in case of a notification of traffic or other incidents likely to cause road blocking and/or severe traffic congestion, in cold winter conditions. When activated, the component will able to deduce an estimate of whether a need for evacuation is required, when and where this should take place, what are the resources required, etc
Prediction sources	The component will use statistical prediction models based on several information sources • Information on traffic incidents, road conditions and environmental conditions disturbing the traffic • Temperature, infra-red and video information from on-the-road sensors • Traffic flow estimation based on recorded data on peak times and zones for traffic congestion • Statistical distribution of fuel reserves in vehicles and when it is likely that vehicles will gradually start to run out of fuel

3.5.4 Privacy & Access Control Enablers

[At this point in research, we find the already given suggestions by FIWARE on GEs to suffice for our requirements]

3.5.5 Ethically Constrained Enablers

3.5.5.1 *Real-time Masking*

Related functionality

Automatic data filtering in compliance with citizens' privacy regulations

Description

The enabler will be used in cases where private and public (i.e. monitored) areas are found very close, resulting to camera sensors acquiring personal images from private places. The enabler will include the following functionalities:

- Awareness of non-authorized to be monitored areas with respect to the sensor's specifications
- Control of the sensor's output and/or operation

In the end the enabler appears to present a protecting mask over said personal data.

Features/ Supported Functionalities

The enabler is going to be composed of the following components, each delivering a respective functionality as presented below:

Component	Functionality
Awareness of Legal Range	The component will keep track of all sensitive positions (altitude, inclination, viewing angle, zoom level, etc) for all deployed sensors and will be used as reference for the overall operation of the enabler. The component will include a password-protected interface for controllers to enter these ranges.
Operation Control	The component will control the motion of the sensor and make sure that this will not violate the thresholds defined in Awareness of Legal Range. This will be useful in cases where C2 operations are trying to control a sensor so as to gain alternative images of the area. The component should recognize this demand and locally examine its possibility. If this should be illegal, the demand will not reach the device and the C2 controller will be informed accordingly, else the command will travel towards the camera sensor as expected.
Output Control	Even in the case that the sensor may acquire images beyond its range the Output Control component will ensure that these images will be lost. The component will assess the sensor's outputs upon device semantics, indicating location in thee dimensions (latitude, longitude, altitude) and inclination across the respective layers. When a value is detected which does not fit the thresholds set by the Awareness of Legal Range component, the Output Control operation will instantly destroy that part of information, making sure that its content will not be access. Example practices could include complex noise, digital key encryption, etc

3.5.5.2 *Personal Data Destruction*

Related functionality

Absolute and permanent destruction of the personal data collected once these exceed their maximum allowed temporal availability

Description

The enabler will be used to ensure complete destruction of the personal data acquired, once these exceed the maximum allowed time limit set to be obeyed for their storage (typically periods last up to 7 days). The enabler will use advanced IT processes to ensure that the personal records are deleted permanently (as opposed to simply erasing data from the disk, which may leave traces for the data to be retrieved. While the Data Destruction enabler will hold a log and a time alarm of the expected destruction phases to take place, the operation will be controlled manually via a user interface.

Features/ Supported Functionalities

The enabler is going to be composed of the following components, each delivering a respective functionality as presented below:

Component	Functionality
Data Log and Reminder	The component will record a brief log of all the personal data being acquired, mainly caring for a) their sensitive nature, b) their date of acquisition and c) their expected date to be erased. Additionally, the component will be aware of any back-ups and copies produced based on auditable records from the database. Accordingly, the component will fire the necessary alarms so as to a) notify which data should be erased and when and b) what copies exist in the system
User Interface	The User Interface component will allow controlling the Data Log and Reminder component, both in terms of criteria (e.g. what threshold time to set as allowed time storage interval) but also to manage the necessity of additionally maintaining personal records under exceptional cases and after acquisition of an according legal decision. The User Interface component will be designed upon high security standards and will allow auditable and dynamic authorized system access
Data destruction	The Data Destruction component will include a set of advanced IT commands to permanently and completely erase data from the system, based upon the locations and file specifications given by the Data Log and Reminder component

4. Ad-Hoc networks

4.1 Introduction

In Public Safety Use Cases Ad-Hoc networks can be used in order to provide reliable support in cases where original network operation is not available. This may be the result of suffering some infrastructure malfunction and/or damage, or even simply caring for connecting to remote areas where no other infrastructures are available. Such cases are proven necessary in situations where urgent and temporal installations of control and command centers in the area need to take place and/or Public Safety teams need to be synchronized, and no main network service is available.

Ultimately, Public Safety procedures need to guarantee full time network support, so as to maintain connection between the C2 centers (data evaluation, decision making and response strategies) with the critical areas being monitored (set of sensors deployed on the field). If the network malfunctions, presents delays or becomes unavailable, this crucially affects the overall efficiency of the entire system.

Public Safety end users often rely on private network providers in order to acquire better performance but also to ensure continuous support. Current private networks can guarantee more than 97% network availability at any case, providing Public Safety end users a reliable interface to operate upon. It becomes therefore apparent that these stakeholders should receive at least these specifications in performance over the public network.

But besides from being a back-up plan for networking, the Ad-Hoc topology is also being applied in routine operations in Public Safety scenarios. Scalability and flexibility are key attributes for Public Safety stakeholders in order to ensure holistic security coverage over a city-wide scale. The assembly of wireless sensors networks, being intelligently triggered by events as well as the communication with mobile units on the move (e.g. police cars monitoring traffic behavior), are both considered important capabilities to be enabled in PS operations.

Ad-Hoc networks rely on wireless networking to overcome distances and physical infrastructures not being available. Network connectivity and availability may be assured by providing capabilities for connecting to different private and/or public networks, also implying the ability of the network to self-adapt to changing topologies. Bio-inspired approaches can provide sustainable support to self-maintained systems, necessary in the development of Ad-Hocs and MANETs[6].

As the nodes in an Ad-Hoc topology increase, crucial challenges regarding the network management (traffic, routing, etc) come to the front. Moreover, security concerns also constitute an important issue to be guaranteed across the Ad-Hoc mode network.

The above challenges may be seen as specific requirements found in each of the main potential scenarios where Ad-Hoc network mode is activated in Public Safety operations, from which we can define the core functionalities necessary for supporting them, as these are defined in Section 4.2 below.

4.2 Key Functionalities in Ad-Hoc Networks

4.2.1 Wireless Sensor Networking

Ad-hoc networks are wireless networks that lack a fixed infrastructure, such as base stations, that form the backbone of standard mobile phone type systems. Instead, the portable nodes that are being used to access the network also act as routers. However, it is possible to deploy infrastructure after a failure –

[6] The BISON Project: Bio-inspired techniques for Self-Organization in dynamic networks, http://www.cs.unibo.it/bison/

one could deliberately place wireless nodes to bridge between areas of fixed connectivity or one could install sensors and bridges in an adhoc manner.

Ad hoc networking clearly requires that the nodes in the system participate in the routing protocol, which must also be highly dynamic, since all nodes in the system may be moving relative to each other, the real radio coverage is not actually circular, and there will be considerable heterogeneity in the system if the system is of any scale. As nodes are destroyed or their power is exhausted, there is a need to reconfigure the system. The need to support different types or different priorities of traffic may also necessitate reconfiguration. Thus, although ad hoc networks are highly survivable and rapidly deployable, since they do not rely on the existence of any particular infrastructure, they are challenging to deal with.

The configuration of an emergency network, dynamically patched together out of surviving infrastructure, may differ substantially from that of normal network operation. Determining, for example, to which sensor node we are talking requires the solution of several problems:

- Sensor node identification
- Address generation
- Dynamic establishment and placement of gateways between different networking technologies
- Labeling of data

Additionally, it would be necessary to ensure machine-to-machine communication capabilities across the devices. Prior to that, we would have to ensure that the positioning of the sensors was in proportion to the signal coverage of each node, while extremely remote areas could be integrated with remote airborne and space-borne infrastructures (e.g. B-GAN). Effective network traffic and bandwidth management protocols would have to be applied in order to coordinate the added nodes, while security protocols would also be necessary to control new additions to the network.

4.2.2 Mobile Command Centre & Mobile units on the move connectivity

The network infrastructure and service providers should enable security access upon authentication, in order to support additional peers to be connected, but without jeopardizing the network's integrity. This would correspond to the case of trying to connect to existing near-by PS network. Otherwise, encryption mechanisms would be required in order to protect the information being handled. Capabilities of seamless network roaming and opportunistic decisions management should be enabled, while support to common public and private networks would be necessary. Again, due to the new network entry and data routing, effective real time management of traffic is required.

4.3 Summary of operational requirements

4.3.1 Wireless sensor networking

- **Extension of nodes** to remote areas
- **Network interoperability** (ability to detect and connect to existing heterogeneous private and public networks)
- Sensor **trans-receiver capabilities**, especially in cases of node failure
- **M2M** communication
- Support to **network traffic and bandwidth control**

4.3.2 Mobile Command Centre

- **Security access upon authentication** to connect additional nodes
- **Encryption** mechanisms
- **Network management and control**. This should be based upon data tagging realized on the sensor level (ref. Situational Awareness) and later allow QoS among different source

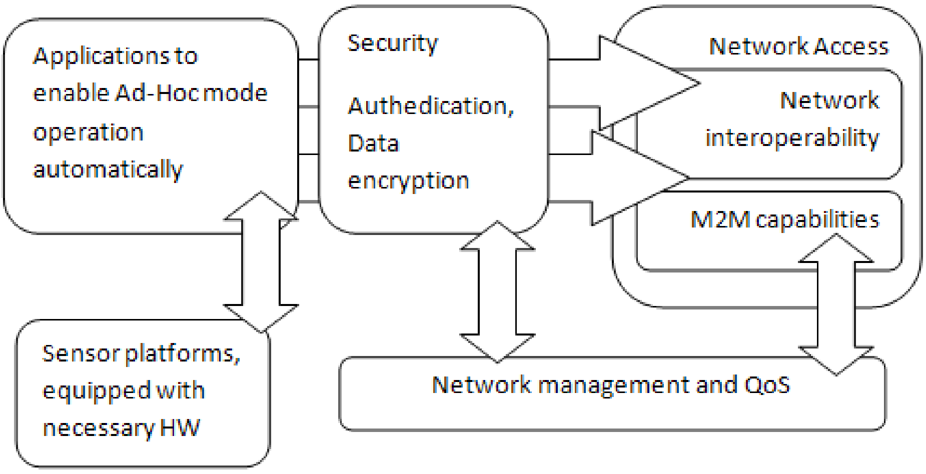

Applications to enable Ad-Hoc mode operation automatically
Security
Authedication, Data encryption
Network Access
Network interoperability
M2M capabilities
Sensor platforms, equipped with necessary HW
Network management and QoS

Figure 1 Mobile Center Information Flow

4.4 Generic enablers to support the Ad-Hoc Operation

Following, we present the Core Platform capabilities that we initially take under consideration in order to deliver the operational requirements posed by the PS end users, as described above. **Table 8** below presents those generic enablers found delivering part or most of the required functionalities. A brief reference of how these enablers are found functionally needed is presented in [2], while future updates of the current document are also expected to deliver more low-level details. Functionalities not delivered by those definitions are explored in the description of new enablers in Section 4.5.

FIWARE reference	Name
4.2.1	Big Data Processing
4.2.2	Complex Event Processing
4.2.3	Multimedia analysis to gather multimedia meta-data
4.2.4	Pre-processing of meta-data during/after gathering
4.2.5	Preprocessing of unstructured data during/after gathering
4.2.6	Localization Platform
4.2.7.	Localisation
4.2.7	Query-access
4.2.8	Publish/Subscribe Broker
4.2.9	Semantic Annotation enabler
4.2.10	Semantic Application Support enabler

Table 8 Core Platform Enablers requested for the delivery of the Ad-Hoc Networks requirements

4.5 Ad-Hoc Specific Enablers

4.5.1 Wireless Sensor Networking

4.5.1.1 *Wireless Sensors Networks*

Related functionality

An enabler to introduce the ability to include wireless communication among channels, so as to favor a city-wide coverage

Description

The enabler will be able to deliver the following functionalities and characteristics:

- Extend some specific sensors (including mobile CCTV cameras, environmental sensors, etc.) to some remote areas in the city where fix ICT infrastructure doesn't exist or it is destroyed

The enabler should be found useful in cases where a destruction e.g. an earthquake has caused the lose of loss of network infrastructures and/or where a city wide coverage has not been accomplished

Features/ Supported Functionalities

The enabler is going to be composed of the following components, each delivering a respective functionality as presented below:

Component	Functionality
Operation Mode Control	The enabler may be required to operate at all times or it might be necessary to be only triggered in cases of an emergency. This feature will allow the enabler to switch the Ad-Hoc operation of the respective sensors on/off in order to save battery life when such connectivity is not required. The feature will be able to detect changes and errors in the network and evaluate a situation of crisis, so as to trigger the Ad-hoc Operation
Traffic control & QoS	It is expected that certain sensors should already be equipped with the necessary HW and SW capabilities to support ad-hoc connection, but the challenge lies on the smooth synchronization of these networks to the main cloud operating. Care needs to be taken so as to not to burden the network (traffic and priorities). The component will look into introducing the ad-hoc nodes to the main cloud effectively, while further managing of the traffic and QoS could be realized with connection to a local Cloud Proxy GE/ Semantic Gateway SE enabled at each ad-hoc area and across the wider network, too
Security and Trust	Similar to the above concerns, this feature will take care of the security and trust challenges arising from the new introductions and changes in the network. Care will be focused on assuring data integrity and reducing data loss, as well as introducing encryption mechanisms for allowing new sensors to enter the respective channels.

4.5.1.2 *Support for airborne communication relay platforms*

Related functionality

Automatic network support for heterogeneous nodes

Description

Airborne communication relay platforms can substantially increase coverage and bandwidth at certain locations. However, it remains yet to resolve challenges of heterogeneity among the different networks. The enabler will support the connection from mobile and static nodes to the existing communication infrastructure, or vice versa, via a heterogeneous airborne relay node. The enabler will be activated and investigate possible relay alternatives whenever the normal communication ways not are good enough. The enabler should support two airborne rely options; Op. 1 amplify and forwarding and Op.2 decode and forwarding.

Features/ Supported Functionalities

The enabler is going to be composed of the following components, each delivering a respective functionality as presented below:

Component	Functionality
Signal Recognition & Authentication	The component will be able to receive and recognize a signal coming from a land/marine source. Taking under consideration the visions for expanding a complex network of fixed and mobile nodes, the component will enforce authentication mechanisms to ensure that the source is secure and validated
Signal Amplification	The component will provide amplification of the received (analogue or digital) signal. The component will also be able to provide signal transformation, i.e. analog-to-digital and vice-versa
Signal Decode/Encode	Signal encoding and decoding will be considered necessary for security and signal processing
Signal Forwarding	The component will be responsible for detecting and validating the final recipient(s) of the signal to be transmitted, establish an appropriate secured communication channel and forward the produced signal

4.5.2 Mobile Command Centre & Mobile units on the move connectivity

4.5.2.1 Mobile Command Centers Connection

Related functionality

An enabler to introduce the ability to maintain communication with mobile C2 in the area at all times

Description

The enabler will be able to deliver the following functionalities and characteristics:

- Connect mobile command centers deployed in the area of the incident even when no communication infrastructures are available.

Features/ Supported Functionalities

The enabler is going to be composed of the following components, each delivering a respective functionality as presented below:

Component	Functionality
Signal Tracking	This component will deliver a similar functionality as the ones presented in Situational Awareness (person/ object tracking). In that sense, the component will recognize the location of the mobile C2 and units in the area, dynamically acquiring their continuous locations and in turn sending a request to the according area nodes
Resources Management & Awareness	The component will be aware of the available ad-hoc nodes in the respective areas, those being defined as sensors or not, public or not, etc. Based on the location of the mobile unit, the component will estimate which node should be activated to be accessed, based on issues of security, range, etc
Automation	The component will try to automate as quickly as possible the access of the ad-hoc networks from the mobile unit. Once these have been activated by the Resources Management & Awareness component, the Automation component will run on the background the necessary QoS and Security protocols for ensuring quick and seamless access

4.5.2.2 Communication with Police Units while on the move

Related functionality

An enabler to introduce the ability to maintain communication across mobile patrols in the area and the main C2 centre at all times

Description

The enabler will be able to deliver the following functionalities and characteristics:

- Full operational communication channels (voice, data access) between Command Centers and Mobile units while they are on the move in the city.
- This should guarantee:
    - Real-time identification of vehicles.
    - Real-time identification and checking of specific people driving a car (police control)

The enabler will allow the immediate feedback from the C2, once the mobile unit has reported a violation. The main communication functionalities shall be ensured by the Mobile Units Connection, while additional functionalities will introduce handling of the private database and secure transmission of the respective messages.

Features/ Supported Functionalities

The enabler is going to be composed of the following components, each delivering a respective functionality as presented below:

Component	Functionality
Standardization	In order to ease and speed-up such processes, the Standardization component will introduce specific values to be entered. This will be linked to the applications running on the police units on the move and to the database structure
Filtering & Masking	The component will introduce a masking/ filtering feature to protect the data being sent across the network from security leakage and unauthorized access, given their sensitive nature
Secure Internal Communication	The procedure of evaluation is to receive some data from the police patrols and compare them internally against a private database. The component will control secure access following pre-define protocols and access levels, will run the requested queries and will forward the final message to the C2 controllers
Secure External Communication	The component will receive a feedback action from the C2 controllers to be forwarded to the mobile patrol unit. The component will follow the necessary security and format transformations for the delivery of the message

5. Command and Control Centers

5.1 Introduction

The Control and Command Center is the core of the Public Safety system network. This is where all the sensor outputs are being stored and analytically processed in order to detect potential threats. It is also here where effective decision making takes place upon the situational awareness acquired (type of threat, location, etc) and the available resources, where response strategies are initiated by the firing of alerts to Civil Protection members in the area, citizens, other PS organizations, etc. Sensor outputs are being acquired and processed with regard to intelligent algorithms and video analytics for the detection of threatening patterns, suspicious behaviors, etc as this has been described in Section 3 – Situational Awareness. At that point alarms are being generated to be further forwarded within the PS network.

5.2 Key Functionalities in Command and Control Centers

5.2.1 Handling of Alarms

First of all, the set of alarms being generated needs to be validated after a true threat detection as opposed to false alarms. This is a significant burden in C2 operations, which could be dealt with, via intelligent processing operations to enable self-learning capabilities in their system. Additionally, in order to avoid detecting threats but upon wrong patterns, cross referencing with third sources can be considered as solution. In order to deal with the amount of false alarms occurring in C2 operations, many end users require a level of flexibility in the trigger of the alarms, allowing both automatic functionalities and human intervention. Therefore, the alarm system must enable a validation option, before the activation alarm occurs including intervention of C2 operators' and cross reference of the detection with other devices.

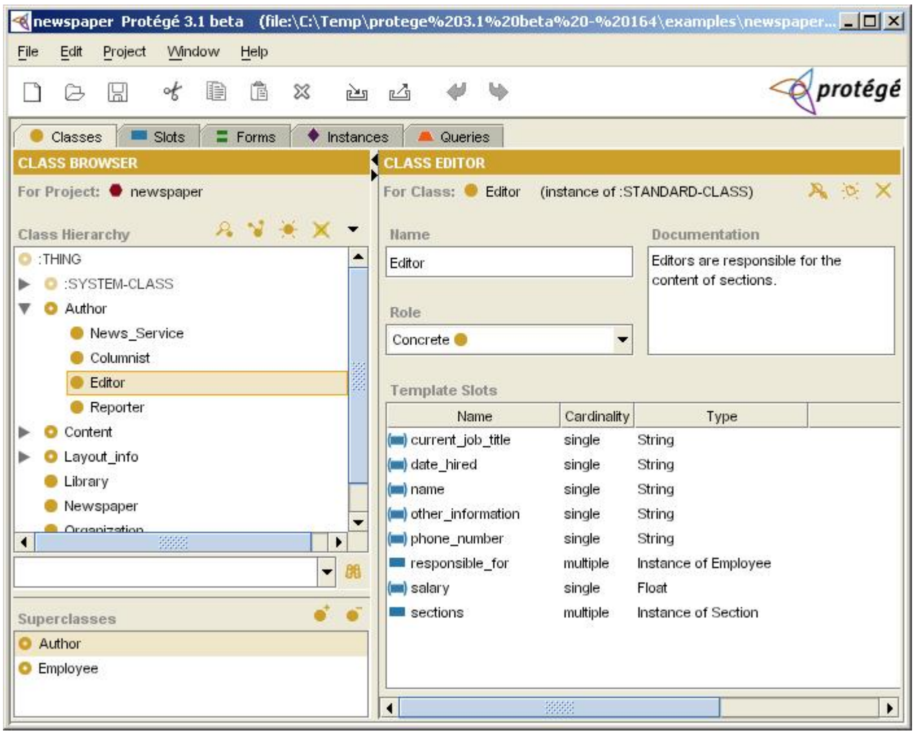
Additionally however, alarm systems should be able to provide a lot of valuable information in order to assist in the process of decision making. Knowing that the original output would have been enriched with meta-definitions and descriptions during process, alarms should to be able to hold some of this information, so as to effectively model a concrete scenario (if any) behind the alarm. For example, in the case when a repetition or pattern of behaviors has been detected, the alarm needs to be modeled with references to previous alerts. Finally, under the category of alarms, alerts must efficiently associate with internal and/or external malfunctions (e.g. an application, a service, a sensor, etc). Such alarms need to be fired quickly, so that the C2 members can take immediate actions to correcting them.

On the other hand, functionalities that allow operators subscribe to some events could be useful. For example, during a police chase the operator can subscribe to all events that involve the stolen car plate in order to tracking it, obviously this functionality requires that sensors notify particular events. This whole functionality could be tackled with Publish/Subscribe Broker GE specified in the Fi-Ware document.

5.2.2 Data Visualization

At this point, flexible graphical interfaces enabling visualization of the images, and also being mapped upon GIS platforms, are required to allow operators to monitor and comprehend the inputs received, as if they were in fact in the place of the incident. These interfaces must **acquire and make full use of informative insights upon the data received** to enable effective decision making and ultimately providing Control and Command upon the situations being monitored .In addition, the visualization interfaces upon which data is being displayed, need to be manageable so as to enable for example zoom in capabilities (according to different levels of information available), fast forward/ record, etc of video streams, manually annotate video images, etc. Data visualization should also be enabled across web interfaces. Web portals could provide real time monitoring of alerts, even for PS members not found in the C2 center, as well as for sharing data alerts during occurrence with other PS organizations. Such web access would of course be defined under strict security protocols.

In the context of PS, it is essential to provide techniques in order to visualize the information in a Semantic manner. The visualization of ontologies is a non-trivial task which involves the following aspects: a) all concepts follow a hierarchy, b) all concepts share relations, c) each concept has various attributes related to it and d) each concept most probably has instances attached to it, which could range from one or two to thousands. Visualizing techniques for ontologies can refer to visualizing the structure of the ontology in order to manage it, or visualizing the historical information (compliant to an specific ontology) in order to understand it: for ontology editing there exist editors, like Protégé, NeOn toolkit or Swoop, which are useful for the Ontology's designer but not for the end user. Below is showed a screenshot of the Protégé Ontology editor (**Figure 2**).


newspaper Protégé 3.1 beta (file:\C:\Temp\protege%203.1%20beta%20-%20164\examples\newspaper...
File Edit Project Window Help
protégé
Classes Slots Forms Instances Queries
CLASS BROWSER
For Project: newspaper
Class Hierarchy
:THING
:SYSTEM-CLASS
Author
News_Service
Columnist
Editor
Reporter
Content
Layout_info
Library
Newspaper
Organization
Superclasses
Author
Employee
CLASS EDITOR
For Class: Editor (instance of :STANDARD-CLASS)

Name: Editor

Documentation: Editors are responsible for the content of sections.

Role: Concrete

Template Slots

Name	Cardinality	Type
current_job_title	single	String
date_hired	single	String
name	single	String
other_information	single	String
phone_number	single	String
responsible_for	multiple	Instance of Employee
salary	single	Float
sections	multiple	Instance of Section

Figure 2 Screenshot of the Protégé Ontology editor

The end user requires the ability to visualize historical information in a useable way, however this information can become very large as well as complex. Therefore an adequate visualization can help humans to work with this information and to understand them more easily. The aforementioned aspects makes it difficult to create a visualization that will display effectively all this information and will at the same time allow the user to perform easily various operations on the ontology. The different approaches for visualizing this information are showed below:

- In the field of ontology visualization, there are several works, mostly in 2D. Apart from these systems that propose visualizations especially tailored for ontologies, there are a number of other techniques, used in other contexts such as graph or file system visualization that could also be adapted to display ontologies. Most of the existing ontology editors use **indented lists**, e.g. Protégé offers a windows explorer-like tree view of the ontology. In this view, the taxonomy of the ontology is represented as a tree (**Figure 3**).

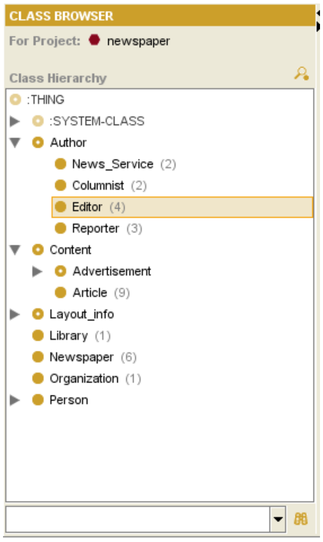


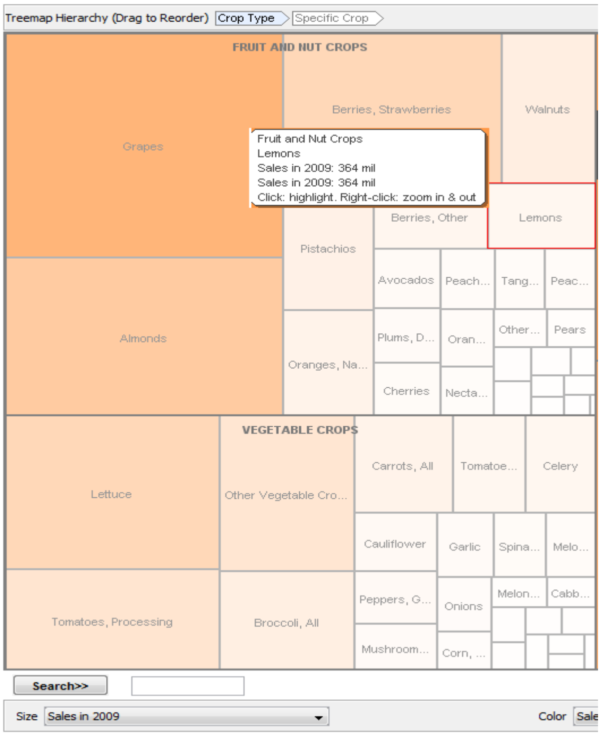
Figure 3 Screenshot of the Protégé windows explorer-like tree view of the ontology

- Other techniques of visualization include ontologies as a set of **interconnected nodes**, presenting the taxonomy with a top-down or left-to-right layout. These nodes can be represented in 2D (e.g OntoViz, IsaViz, SpaceTree) or in 3D (Cone Tree, Tree Viewer, OntoSphere). This category normally is well-known like Node-Link and tree

- **Zoomable visualizers** group all the methods that present the nodes in the lower level of the hierarchy nested inside their parents and with smaller size than that of their parents. These techniques allow the user to zoom-in to child-nodes, making them the current viewing level. As well the previous techniques, the information can be represented in 2D (e.g. Grokker, Jambalaya, Cropcircles) or in 3D (e.g. Information Cube, Information Pyramids, Gropher VR)

- The **space filling** techniques are based on the concept of using the whole of the screen by subdividing the space available for a node among its children (**Figure 4**). The size of each sub-division corresponds to a property of the node assigned to it, e.g., number of contained nodes, size, etc. In 2D highlights Treemaps can show attributes of leaf nodes by size and color-coding. Treemaps enable users to compare sizes of nodes and of sub-trees, and are especially helpful in revealing patterns

- Finally, other visualizations techniques apply **sophisticated transformation** in order to show the information. This group of techniques is based on the notion of distorting the view of the presented graph in order to combine context and focus. The node on focus is usually the central one and the rest of the nodes are presented around it, reduced in size until they reach a point that they are no longer visible. Usually a hyperbolic equation is used to this end. The user has to focus on a specific node, in order to enlarge it. Similar to the previous techniques can be represented in 2D (OZONE, OntoRama, MoireGraphs, TGVizTab) or 3D(**Figure 5**)



Fruit and Nut Crops
Lemons
Sales in 2009: 364 mil
Sales in 2009: 364 mil
Click: highlight. Right-click: zoom in & out

Figure 4 Space Filling Ontology Visualization technique, California Crop Sales in 2009 using the tool ManyEyes

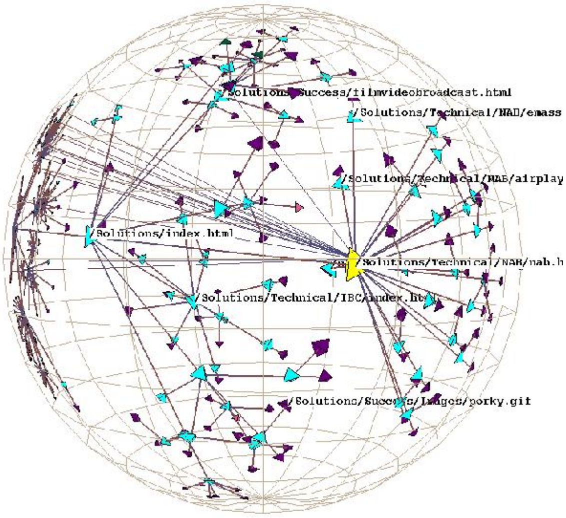

/Solutions/Success/filmvideobroadcast.html
/Solutions/Technical/NAD/emass
/Solutions/Technical/NAB/airplay
/Solutions/index.html
/Solutions/Technical/NAB/nab.h
/Solutions/Technical/IBC/index.htm
/Solutions/Success/Images/porky.gif

Figure 5 3D Hyperbolic Tree

5.2.3 Management Capabilities

As mentioned in Section 3 – Situational Awareness, Sensitive data are being stored and therefore demand the development of secure management mechanisms, being accessed only via private network services, i.e. being away from the public network. Apart from the security considerations, the C2 databases require complex data management systems to handle a vast amount of demanding data, coming from various sources. Interoperability of these systems is also required, when dealing with different sensor outputs and specifications; Semantic annotations could contribute on the data synchronization, however more advanced rules need to be defined so as optimize dynamic file allocation.

Management capability systems must enable C2 members to achieve full management of data storage and ICT requirements of each application running across the network and manage network traffic and ensure high levels of QoS, based upon considerations such as a) changes in priorities, b) network malfunction, c) temporary loss of resources, etc. Accordingly, C2 operations need to include interfaces with specialized APIs to enable management of the equipment capabilities. Operators need to be able to adjust the information being displayed in terms of managing the sensor operation on the field, remotely. For example, C2 end users require being able to adjust the pan zoom and direction of a camera, the tracking of a given object/ person, etc across the series of the sensor network (tracking), etc.

All the aforementioned managing capabilities are of course considered being enabled on demand. Focusing on the Semantics, C2 also needs a tool for the management of the Ontology, which must be shared by all actors in the PS. A key aspect on ontology management is the storage and retrieval of ontologies. This issue requires the development of ontology management systems, responsible for ‘semantic’-based ontology storage. Efficient re-usage of knowledge in a closed context requires a library system for ontologies. An ontology management system should take care of storage, identification, edition, and retrieval of ontologies used for similar applications. Ontology library systems are an important tool to group and re-organize ontologies for further reuse, integration, maintenance, mapping and versioning.

Most ontology storage systems have either a client/server-based architecture aiming for remote accessing and collaborative editing (e.g. WebOnto[7], DAML Ontology Library[8], OntoLingua[9], Protégé) or a Web accessible architecture (e.g. SHOE[10], IEEE SUO[11]). The Ontology Server has a database-based architecture. Most of the ontologies are classified or indexed. They are stored in the modular structured library (or lattice of ontologies). WebOnto, OntoLingua and ONIONS all emphasize the importance of modular structure for ontology library system, which pave the road for the reuse of ontology, management of ontology, reorganization of ontology library system. A detailed report on several of the available tools may be found [12], while the most prominent candidates for use in the context of PS are shown below:

- **Sesame**[12] is an open source RDF framework with support for RDF Schema inferencing and querying. Originally, it was developed by Aduna (then known as Aidministrator) as a research prototype for the EU research project On-To-Knowledge. Now, it is further developed and maintained by Aduna in cooperation with NLnet Foundation, developers from Ontotext, and a number of volunteer developers who contribute ideas, bug reports and fixes. Sesame has been designed with flexibility in mind. It can be deployed on top of a variety of storage systems (relational databases, in-memory, file systems, keyword indexers, etc.), and offers a large selection of tools to developers to leverage the power of RDF and RDF Schema, such as a flexible access API, which supports both local and remote (through HTTP or RMI) access, and several query languages, of which SeRQL is the most powerful one. There is a Protégé plug-in for Sesame, but not very actively developed

[7] http://kmi.open.ac.uk/projects/webonto/

[8] http://www.daml.org/ontologies/

[9] http://www.ksl.stanford.edu/software/ontolingua/

[10] http://www.cs.umd.edu/projects/plus/**SHOE**/

[11] http://suo.ieee.org/

[12] http://www.openrdf.org/

- **Jena**[13] is a Java framework for building Semantic Web applications. It provides a programmatic environment for RDF, RDFS and OWL, SPARQL and includes a rule-based inference engine. Jena is open source and grown out of work with the HP Labs Semantic Web Program. Jena2 is the second generation of the Jena toolkit. It conforms to the revised RDF specification, has new capabilities and a new internal architecture. A design principle for Jena2 was to minimize changes to the API from Jena to Jena2. The Jena database subsystem implements persistence for RDF graphs using an SQL database through a JDBC connection. Jena has also been integrated in Protégé-OWL [14]. It includes:
    - A RDF API
    - Reading and writing RDF in RDF/XML, N3 and N-Triples
    - An OWL API
    - In-memory and persistent storage
    - A SPARQL query engine

There are other **commercia**l tools like the ones created by Oracle, Mondeca and Ontoprise. We present them here as an example of the tools available commercially that will be taken into account:

- **Oracle's** proposal stores RDF triples in the Oracle database as a logical network (using the Oracle Spatial Network Data Model)[15]. Oracle 10g supports directed and un-directed logical graphs (networks) as part of Oracle Spatial Network Data Model (NDM). The proposed RDF data model maps RDF triples to a logical network managed by NDM. In addition to the core data, a catalogue service is provided: by maintaining information about different RDF models, including the namespaces used in these models. RDF triple data is mapped onto a graph by storing subjects and objects as nodes, and properties as links. The storage for RDF data is managed by Oracle: all the RDF data is managed in a central schema, and user-level access functions and constructors are provided to query and update the RDF data. There is one universe for all RDF data stored in the database. Each RDF triple: {subject, property, object} is treated as one unique database object. As a result, a single RDF document comprising a number of triples will result in multiple database objects. Oracle also offers a sample Protégé plug-in for its RDF store
- **Mondeca ITM e-Knowledge**[16] is a knowledge representation management application based on Semantic Web technology (Web 3.0) and ontologies. With a complete modeling capability according to the area of activity, the tool enables all types of concepts to be described and organized into classes, and all types of relationships between concepts to be managed, ensuring rapid deployment of an operational solution that is perfectly suited to the specialist domain. Designed for the web and for SOA (service-oriented architecture), the tool enables advanced information access and processing services to be offered to users, and also the construction of automated services using web services
- **OntoPrise OntoStudio**[17] is a professional development environment for modeling ontologies and administrating ontology-based solutions that allows for the integration of multiple heterogeneous data sources. The product is based on a modular design and supports the

[13] http://jena.sourceforge.net/

[14] http://protege.stanford.edu/plugins/owl/jenaintegration.html

[15] www.oracle.com

[16] http://www.mondeca.com/index.php/en

[17] http://www.ontoprise.de/content/e1171/e1249/index_eng.html

development of defined modules as well as use-based customization. Eclipse, the open source editor framework, provides the implementation base for the product

The use of the appropriate ontology storage module is essential in the context of PS. The aforementioned options will be thoroughly investigated as to their effectiveness, compatibility with other selected tools, robustness and support. Ontology storage evaluations for Large OWL Dataset[18] will be also taken into account. The maintenance of Ontology should be carrying out using a tool that checks the consistency of the Ontology. This maintenance is mandatory because of is quite complex define a complete Ontology from scratch, therefore an incremental approach should be adopted. The reasoner engine are going to infer new knowledge from previous stored one, these inferences require a set of rules (inference rules) or axioms, (e.g. two different events that involves the same car plate are related, independently of the place that occurs), because these rules or axiom can change over the time a tool for management rules is highly recommended. Moreover taking into account that the number of new events in SafeCity grows at rate of 432GB per day (see D3.1), features for Big Data Analysis are mandatory.

5.2.4 Data Integration and Interoperability

Data being forwarded to the C2 center are being acquired from a variety of different sensor providers, data types, location, situation, etc. In order to effectively assess the set of information received holistically, it is required:

- Data fusion techniques to deal with the integration of data and related heterogeneity constraints
- Interoperability capabilities across the communication of multiple PS organization, e.g. fire department, CDC, police stations, etc. As mentioned above each organization needs to maintain private clouds for storing their databases under secure and private networks. However, PS organization often need to communicate and synchronize their activities, share alerts and mutually define activities to be followed
- Data **interoperability capabilities also in the cases of receiving citizen information**, e.g. video footage from a scene captured by a mobile phone
- **High security mechanism and authentication procedures** being enabled on a subsidiary intercommunication platform, suggested by **connectivity requirements among the different private networks**
- **Establishment of common frameworks for defining and describing sensor inputs**
- **Data standardization and integration** procedures to enable uninterrupted processes

5.2.5 Unified Emergency Responses

The Unified Emergency Response services may be deployed, for instance, at a city level, where multiple PS organizations could be involved: City Police, National police attending the corresponding city, Fire Brigades of different parts of the city, Medical services managed by public authorities, other medical services as Red Cross, etc. These services must allow:

- A holistic awareness of the threats defined to C2 end users and the available resources for dealing with them. C2 operators need to be aware at all times of the available services, mobile units, emergency equipment and so on, able to applied if necessary

[18] Y. B. Guo, Z. X. Pan, J. Heflin, An Evaluation of Knowledge Base Systems for Large OWL Datasets, in Proceedings of the Third International Semantic Web Conference, Hiroshima, Japan, November 7-11, 2004

- Awareness of both the resources of the C2 center alone, as well as of other PS organizations' with which the center cooperates
- The common Emergency Centre of the city may to behave as the one which provide the on-line and secure service to the other organizations. All entities involved feed the application with available PS resources, major plan events that will taking place, ad-hoc security procedures of each critical infrastructure and its relevant information (emergency exists, maps of the place or CI, etc.), surveillance data alerting with incidents occurrence, etc, potential risks in the area
- Automated processing for decision making and best opportunistic plans based upon the situation severity and characteristics and PS organization capabilities
- To provide these share-based customized tools to public safety and security organizations within a city, within a region, within a state or even among European organizations in case of necessity. For instance, if the response services are handled within a city, the common Emergency Command Centre holds governance and operational responsibility for the Emergency Response software tools and the rest of PS organizations interested can securely access the cloud-based, on-demand service

5.3 Summary of operational requirements

5.3.1 Handling of Alarms

- **Validation** of the threat
- **Cross-reference** of the threat detection **with third sources**
- **Self –learning** capabilities on C2 system
- Level of **flexibility** in the trigger **of the alarms** to end users

5.3.2 Data Visualization

- **Graphical interfaces** including visualisation of images on GIS platforms
- Ability on C2 operators to **manage visualisation interfaces**
- **Web interfaces and portals**
- **Visualization of semantic information**
    - **overview-detail views:** users expect to have on the one hand a good overview and on the other hand to see the instances in the context of the whole ontology. Additionally it is important to see fast how many instances a class has
    - **browsing and updating:** users expect that a visualization should allow for browsing, adding and removing elements inside the ontology or to have the possibility to hide/show elements. Furthermore, it should be possible to switch between different classes as well as instances inside the ontology
    - **easy to learn and understand**: a visualization should be easy to learn and to use. Furthermore, the aspects "simplicity, readability and flexibility" should be considered
    - **structure/ relationships views**: users expect that the hierarchical structure should already be evident by the design of the visualization layout. Additionally, it is necessary to see very fast the taxonomy information with all its detail information and the relevant relationships between them
    - **performance**: users expect a good solution in regard to very large ontologies
    - **search**: Few users explicitly state that they would like to have a search to find specific elements and this requirement is considered mandatory
    - **manual annotations**
    - **adequate user interface,** showing matching as well as related elements
- **Management of semantic information**
    - Supporting ontology reuse by **open and central storage, identification and versioning**
    - Supporting ontology reuse by **providing smooth access to existing ontologies** and by **providing advanced support in adapting ontologies** to certain domain and task specific circumstances (instead of forcing to develop such ontologies from scratch)
    - Supporting ontology reuse by fully employing the power of **standardization**. Providing access to standardized upper-layer ontologies and representation languages is one of the main steps in bringing knowledge sharing and reuse to its full potential

5.3.3 Management Capabilities

- **Secure management** mechanisms to support sensitive data
- Data management systems able to **handle a vast amount of demanding data**
- **Interoperability of the management system**
- **Management of network traffic** e.g. changes in priorities, network malfunction, temporary loss of resources
- Tool for the management of the **Ontology (manual semantic annotations)**

5.3.4 Data Integration & Interoperability

- **Data fusion** techniques to deal with the integration of data
- Interoperability capabilities across the communication of **multiple PS organizations** and in the cases of receiving **citizen information**
- High **security mechanism and authentication procedures**
- **Data standardization** and integration

5.3.5 Unified Emergency Responses

- **Awareness of available resources** for dealing with detected threats
- **Awareness** as well as **of the resources of other PS organizations**
- The ability to **the common Emergency Centre** of the city to behave as the one which provide the on-line and secure service to the other organizations
- **Automated** processing for **decision making**
- To provide **share-based customized tools** to public safety and security organizations

5.4 Generic enablers to support the C2 Operations

Following, we present the Core Platform capabilities that we initially take under consideration in order to deliver the operational requirements posed by the PS end users, as described above. **Table 9** below presents those generic enablers found delivering part or most of the required functionalities. A brief reference of how these enablers are found functionally needed is presented in [2], while future updates of the current document are also expected to deliver more low-level details. Functionalities not delivered by those definitions are explored in the description of new enablers in Section 5.5.

FIWARE reference	Name
3.2.1	IaaS DataCenter Resource Management
3.2.2	IaaS Service Management
3.2.5	Cloud Edge
3.2.6	Monitoring
3.2.7	Resource Metering and Accounting
4.2.1	Big Data Processing
4.2.2	Complex Event Processing
4.2.3	Multimedia analysis to gather multimedia meta-data
4.2.4	Pre-processing of meta-data during/after gathering
4.2.6	Localization Platform
4.2.7	Query-access
4.2.8	Publish/Subscribe Broker
4.2.9	Semantic Annotation enabler
4.2.10	Semantic Application Support enabler
4.3.1	Social Network Analysis
4.3.2	Mobility Analysis
4.3.5	Opinion mining
5.2.4	Service Registry
5.3.5	Service composition editor
5.3.6	Execution engine
5.3.7	Mashup execution engine
5.3.8	Service composition engine
5.3.9	Service orchestration engine
5.3.10	Aggregator repository
5.4.1	Data Mediation
5.4.2	Protocol Mediation
5.4.3	Process Mediation

6.2.1	IoT Communications
7.2.2	Cloud Edge
7.2.2	Cloud Edge
8.2.1	Security monitoring
8.2.2	Identity Management
8.2.3	PrimeLife Policy Language (PPL) Engine
8.2.4	Identity Mixer (IdeMix)
8.2.5	Context-based security and compliance
8.2.6	Optional Security Service Enabler

Table 9 Core Platform Enablers requested for the delivery of the C2 Centers requirements

5.5 C2 Specific Enablers

5.5.1 Handling of Alarms

5.5.1.1 *Incident Detection Indicator*

Related functionality

Automatic (i.e. including minimum human intervention) identification of alarms (detection of an alarm and recognition of its nature), threat validation

Description

While key processing capabilities enabling minimum human intervention in the definition of alarms were presented in Section 3- Situational Awareness, the enabler looks into the handling of false alarms, the rate of which is quite often significantly high and burdens the organization's resources.

The enabler will be able to deliver the following functionalities and characteristics:

- Minimum human intervention for detection of an incident.
- Machine capabilities for extracting relevant and meaningful semantic descriptions of objects and citizens behaviors for aiding decision-making and situation assessment.
- Alarm handling, filtering and correlation: Define individual/several alerts for a predefined area, or even for each of the deployed cameras.
- Alarms centralized management.
- Event-trigger support: Integrates with alarm, process control, and other systems

Features/ Supported Functionalities

The enabler is going to be composed of the following components, each delivering a respective functionality as presented below:

Component	Functionality
Cross-Checking	The component will search based upon timestamp, location and other semantics the related sources and messages, concerned with an alert. Based on this information, the component shall mark the possibility of an alert being true or false, based upon the common patterns found in multiple sources. Additionally, the component will look independently the occurrence (i.e. frequency) of the alerts fired per source. Finally, comparison with learned-by-lessons mistakes and success stories will also be used as reference
Validation	The component will hold multiple capabilities depending upon the nature of the alarm. This would be rather necessary both in cases of regular sensor monitoring as well as in the cases where citizens enter alerts from a city-installed access point. The main tools for examining the validity of the alert would be • Number of cross-checked sources • Standardization – complete fill with the accepted values of the respective fields expected for each signal type • Identification of source – sensor, citizen, operator; in the case of manual annotations, an identification of certain details should suffice in assuring validity; in the case of automated processes, the component should look for potential recorded errors in the system, i.e. is this sensor operating normally?

Prioritization & Management	The component will acquire information from the respective sources upon the level of the possibility of the threat (i.e. probable, possible, certain, etc). This information will also be used in combination with the Cross-Checking component; the second will in fact be necessary in cases where the first meta-information is not available. The component will then, being aware of the set of different alerts recognized, forward the set of alarms the respective applications (see enablers below) for them to be further forwarded to the final recipients. The user could introduce filters to exclude for example the triggering of alarms marked as having very low possibility of occurring

5.5.2 Data Visualization

5.5.2.1 Common Operating Picture (COP)

Related functionality

Advanced interactive user interfaces for online and offline holistic data analysis

Description

The enabler will be able to deliver the following functionalities and characteristics:

- COP for each specific city providing a geo-spatial map of that city with various map layers: street names, cameras positioning, sensor locations, units deployed etc.
- Click and zoom over any region of the map.
- Click on the camera to watch live video displayed.
- Integration of information across various city agencies departments.
- Multi-source data-fusion.

Features/ Supported Functionalities

The enabler is going to be composed of the following components, each delivering a respective functionality as presented below:

Component	Functionality
Data Management	The component will integrate all sensor inputs and make them available to the enabler, filtering and categorizing them intelligently upon a) type, b) sources, c) area, etc. In fact, user specifications upon the different layers that the operators would like to choose from can be used as additional categorization criteria. The component should be able to access current (real-time) and recent (across a defined time span) data.
Standardization	The component will take care in assuring that the different sensor inputs acquired can be displayed under a common interface by standardizing them across the interface’s design and their contextual semantics
GIS mapping	The component will enable the provision of a GIS interface based on real-life location information of the area(s) being monitored. The interface will enable zooming in/out capabilities, navigation options and the display of different layers (e.g. environmental sensors, video cameras in central square, etc).
Video Management	Due to their demanding nature, this component will support the Data Management feature, which is expected to act more as an integrator, so as to handle real-time management of multimedia in the user interface. Functionalities will include appropriate compression rate, easy and efficient management capabilities (play, resume, retrieve next camera, etc)

5.5.2.2 Public Spaces Visualization

Related functionality

Ability to acquire inputs from CCTV cameras towards creating life-like simulations of the area being monitoring (3D representation on buildings and persons, clear reference on street names, etc)

Description

Public Spaces Visualization integrates all sum of sensors deployed and expands to a broad category of applications. Although there exist several functionalities, like the ones described in the Situational Awareness Section, which are more specific and oriented upon the detection of specific threats the enabler holds more generic functionalities found to be necessary in most Public Safety Multimedia Applications, e.g. tracking capabilities.

The enabler is in this sense composed of key functionalities mainly focusing on user interface capabilities, while the enablers defined in 3.5 focus on dedicated scenarios while making use of the enabler as a key reference in development. The enabler will be able to deliver the following functionalities and characteristics:

- Multiple web-based consoles to configure, manage, display, and control video throughout a customer’s IP network
- Integration of stationary and mobile cameras information.
- Video from any camera can be directed to any monitor or a video wall.
- Tracking suspicious target from one camera to another camera.
- Scheduled and event-based video recording
- “Record Now” feature while viewing live video
- Event setup and event notifications
- Authentication management features to access to different cameras or recorded video.
- Remote viewing access through internet browser (password protected).
- Web-service based intuitive interface
- Location of different public safety agents around the city (resources status and location)

Features/ Supported Functionalities

The enabler is going to be composed of the following components, each delivering a respective functionality as presented below:

Component	Functionality
Area Display Management	The component will provide a map of the monitored area of the city with 2D (and 3D) views. This module will offer zoom capabilities and possibility to change the view to 2D to 3D once the zoom level is big enough. CCTV cameras, archived images and 3D modeling are going to be used in the visualization. The enabler will also offer the ability to register a background image/frame of a scene, potentially with the manual intervention of a user.
Video management	The component will allow the controller to choose from the available sensors which video image he wishes to study. The component can in fact deliver intelligent support by understanding basic meta-information (alert or not, timestamp, location, etc) and suggest to the controller additional video images. Finally, the component will force a security wall to certain video images to be protected by non-authorized access. This could be automatically (recognizing the user profile) or by requesting login access at the sensitive points

Remote sensor control	In order to enable tracking capabilities, it becomes often necessary to alter with the camera's settings (angle and direction). Additionally, in order to acquire different levels of details, detect crowd vs. persons, etc it is also required to manage the video's zooming capabilities. This module will offer the capability to remotely control CCTV sensors, ask for stream transmission, and control Pan/Tilt/Zoom commands
Content Management	This feature will allow the ability to replay part of a video input based upon specific requirements such as starting date, duration, sensor identifiers, etc, so as to ease the C2 evaluation of the video images upon request
Online Management	The component will constitute an online visual interface holding the overall capabilities of the enabler, under the development of the necessary interface. For example, extra security measures will be forced (password encrypted, data filtering, etc). Access through private only or not network should be chosen upon the user's requirements

5.5.3 Management Capabilities

5.5.3.1 Management of Video Stored Information

Related functionality

Processing capabilities dealing with data storage and retrieval efficiency for effective handling of vast amount of demanding data

Description

The enabler will be able to deliver the following functionalities and characteristics:

- Real-time storage process.
- Dynamic Security authentication management features to access to recorded video.
- Dynamic file allocation optimizing disk usage for stored video.
- Encoding video to save space in disk.
- Standard video compression algorithms such as MJPEG, MPEG-2, MPEG-4, and H.264.
- Event-tagging of video for review and archival purposes.
- Redundant archives: Flexible archiving of video at multiple locations, frame rates, and durations.
- Record and view simultaneously.
- Possibility of simultaneous agents viewing live or recorded video at same time.
- Video stored capacity up to 7 days for all cameras.

Based on the above considerations, the enabler should be hosted on a cloud service and deliver the aforementioned functionalities to the framework. In that sense, some basic storage and management capabilities (dynamic storage, dynamic allocation, log, disk storage optimization, standard compression, etc) are found able to be covered by FIWARE's CH3 and CH4 enablers.

Features/ Supported Functionalities

The enabler is going to be composed of the following components, each delivering a respective functionality as presented below:

Component	Functionality
Dynamic secure access	The component will deliver the ability to accommodate different levels of access to the database, based upon a) the content of the data and b) the source making the query. The component will be designed upon the legal and ethical frameworks obliging PS organizations to protect personal data. The component will integrate functionalities such as • Password secured data • Different authentication profiles • Banning external access, i.e. enabling only internal private network access, for the protection of the sensitive data
Data Destruction	The component will be triggered after the allowed duration for storing personal data (typically for PS organizations ~ 7 days) and will initiate a set of processes to ensure that data has been lost. Personal data need to be handled with extra care and typical erase actions which do not assure the absolute loss of data from the disk would not suffice

5.5.4 Data Integration & Interoperability

[At this point in research, we find the already given suggestions by FIWARE on GEs to suffice for our requirements]

5.5.5 Unified Emergency Response

5.5.5.1 *Unified Incident Management (Public Safety Resources)*

Related functionality

Awareness of available resources and coordination interface among PS authorities

Description

The enabler will be able to deliver the following functionalities and characteristics:

- Smart resources Management: Depending on incident, a suggestion of the number of units necessaries to solve the problem (fight-fighters, polices, medical units).
- Indication how public agencies should act and where the resources should be deployed.
- Inter-agencies allocation.
- Direct contact with units deployed in the incident area providing them with the procedure to be followed.
- Transfer of control and monitoring to any other point in the network in an emergency situation
- Ability to manage devices and alerts from a centralized location
- Ability for products from various vendors to interoperate in the same network
- Usage of an open, standards-based infrastructure.

Features/ Supported Functionalities

The enabler is going to be composed of the following components, each delivering a respective functionality as presented below:

Component	**Functionality**
Decision Making Support System	The component will be used to acquire dynamic information upon the event occurring, from the moment of the alert detected and first immediate response, to its final resolution. The component will receive inputs upon the location of the area and key infrastructures/ places, involved persons (citizens passing by, criminals if applicable), available forces from different PS organizations.
Intelligent Adaptability	The component will be composed of a cluster of intelligent algorithms and agents to support the operation of the Decision Making Support System and to enable its adoptability and learned-by-lesson behaviors
Real-time updated secure database	The component will be composed of a real-time updated database which will automatically share information from different units based on a) their available resources and b) their inputs and feedback on the event. Due to the necessity to allow external communication, the database will be secure heavily with protocols and encryption mechanisms (perhaps also looking into onion structures for secure messages)

6. Alerting Technologies

6.1 Introduction

Alerting Technologies are concerned with in time informing citizens upon threats occurring in monitored areas. Examples of such operations may include light management patterns and urgent road messages (e.g. «Use the right lane», etc) on traffic-related incidents, or even instruct citizens to evacuate a critical site. Alerting messages can either inform citizens upon on-going or upcoming threats.

The operation could be designed to take place as a solely (or almost entirely) automated process, with limited human intervention, mostly being necessary in cases where threats, and accordingly alerts, escape routine situations, common/ already seen scenarios, etc**.** However, taking under consideration the high amount of false alarms noted in C2 applications raises the concern that we cannot risk sending automatically false alerts to citizens as they would a) be massively conquered by an imagery threat in every such situation and b) eventually disregard such notices, thinking that they are faulty and unreliable.

We consider the following main scenarios involving citizen alerts, once a human operator has initiated this process:

- Alerting citizens in the area, via deployed infrastructures
- Alerting citizens via web interfaces
- Alerting citizens via mobile networks
- Alerting citizens via media

6.2 Key Functionalities in Alerting Technologies

According to the description of alerting technologies introduced above, we propose that alerting technologies should enable:

- Automation up to the level of modeling the alerts and submitting them after a human trigger has been enabled
- Automatic models for the shaping of the alert (content and context) designed upon pre-defined meta-data definitions, upon which threat detection is also being realized
- Automation can exist on the definition of recipients and on reaching their devices.
- The ability to connect to multiple private and public networks, for reaching out to citizens, media, etc
- Manipulation of infrastructures already being used in the area in order to serve in addition alerting operations. For example, CCTV cameras can be connected with controlled microphones producing a given signal. The signal could be a concrete message, e.g. «Please leave this area for your safety» or transmit a sound code, e.g. a combination of distinct beeps, to be interpreted by PS units on the field who can then alert and help citizens in the area. Another example includes controlled traffic light management in traffic sensors or even concrete signaling, informing upon ongoing (e.g. an accident has occurred) and/or upcoming (e.g. severe weather conditions with risk to jeopardize the road consistency) threats
- The ability to instantly inform a vast amount of users upon a threat through online social networking Users in this case are expected to be followers of the specific network, i.e. they need to have already been aware of the service and have subscribed to that. Such online

societies can also guarantee data integrity by allowing sharing information only amongst their users

- The ability for citizens to subscribe to a mobile network service provided by PS organizations to instantly receive notifications upon a specific area and/or the area they are found (location awareness, etc). Additionally, alerting mechanisms could directly communicate with cellular phone services providers and transmit messages to all subscribers found within a given cell

- The ability to inform citizens via media either automatically (directly submitting pre-defined model of message – e.g. an email ,media report- to pre-defined media receivers) or via human intervention

- Messages including information about the type of threat, timestamp, location, severity/possibility level and actions to be realized by citizens in the area. The above should be defined upon the meta definitions of the SafeCity framework, which should among others include behavioral protocols for citizens instructions

- Definition of the position of the threat in terms of cellular networks divisions keeping a database of citizens willing to received PS alerts

- Automatic web updates

6.3 Summary of operational requirements

- Light management patterns and **urgent road messages**
- **Limited human intervention** along with minimal possibility of false alerts
- **Automated modeling of alerts**
- **Automatic definition of the receivers** of the alerts
- Connection to **multiple networks**
- **Serve additional alerting operations** in the existing infrastructures
- Inform **a vast amount of users** upon a threat **through online social networking** and web updates of the services
- Inform **a vast amount of users** upon a threat **through mobile service subscription** and definition of the threat on terms of mobile network divisions
- Inform **a vast amount of user**s upon a threat **through media** automatically or not
- Maintain **database of citizens willing to receive alerts**

6.4 Generic Enablers to support Alerting Technologies Operation

Following, we present the Core Platform capabilities that we initially take under consideration in order to deliver the operational requirements posed by the PS end users, as described above. **Table 10** below presents those generic enablers found delivering part or most of the required functionalities. A brief reference of how these enablers are found functionally needed is presented in [2], while future updates of the current document are also expected to deliver more low-level details. Functionalities not delivered by those definitions are explored in the description of new enablers in Section 6.5.

FIWARE reference	Name
4.2.1	Publish/Subscribe Broker
7.2.4.	Service, Capability, Connectivity and Control (S3C)

Table 10 Core Platform Enablers requested for the delivery of the Alerting Technologies requirements

6.5 Alerting Technologies Specific Enablers

6.5.1.1 *Alert Activation through fix mobile networks*

Related functionality

<u>Enabling the automatic transmission of alerts through landline infrastructures</u>

Description

The enabler will be able to deliver the following functionalities and characteristics:

- Alert to other Public Safety agencies (police, medical services, fight-fighting) giving notification of a specific incident and even indicating how proceed
- The alerts can be sent to the entire network or a targeted group depending on need

Features/ Supported Functionalities

The enabler is going to be composed of the following components, each delivering a respective functionality as presented below:

Component	Functionality
Intelligent Recipients Awareness and Management	The component will recognize based on the nature of the alert which recipients should be specified (e.g. police units, ambulances, fire department, etc). Also, the component will estimate location parameters and available resources

6.5.1.2 *Alert Activation through Mobile Phones*

Related functionality

Enabling the automatic transmission of alerts through cellular telephony networks (e.g. in the form of text message - SMS)

Description

The enabler will be able to deliver the following functionalities and characteristics:

- Alert to other Public Safety agencies (police, medical services, fire-fighters) giving notification of a specific incident and even indicating how to proceed
- The alerts can be sent to the entire network or a targeted group, depending on need

Features/ Supported Functionalities

The enabler is going to be composed of the following components, each delivering a respective functionality as presented below:

Component	Functionality
Recipients Awareness and Management	The component will hold track of the users who wish to accept alerts and their according details (contact information) as well as criteria. For example, a citizen wishes to be informed of an alert in town close to his house, a user wishes to be alerted of an event only when he is absent, etc. The component will keep track of their preferences and will enable define the final lists and channels of recipients to be informed. In order to accomplish that, the component will keep track of the users' position across their cellular network in order to define her location and her potential interest in receiving an alert. All the above will be realized with the users' consent

6.5.1.3 Alert Activation through Internet Networks

Related functionality

Viral alerting of citizens and PS members through online social networks (offering global coverage and full time support)

Description

The enabler will be able to deliver the following functionalities and characteristics:

- Alert to population on a specific event through social networks as TWITTER or FACEBOOK
- Instant message (IM) or short message service (SMS)
- Alert to other Public Safety agencies (police, medical services, fight-fighting) giving notification of a specific incident and even indicating how proceed
- The alerts can be sent to the entire network or a targeted group depending on need

Features/ Supported Functionalities

The enabler is going to be composed of the following components, each delivering a respective functionality as presented below:

Component	Functionality
Recipients Awareness and Management	The component will hold track of the users who wish to accept alerts and their according details (contact information) as well as criteria. For example, a citizen wishes to be informed of an alert in town close to his house, a user wishes to be alerted of an event only when he is absent, etc. The component will keep, after the users' consent track of their preferences and status, and will enable define the final lists and channels of recipients to be informed
Web Announcement Management	The component will be responsible for forwarding the related information to the respective channels, but is shall also look into challenges of security and social implications, i.e. controlling how viral an alert becomes and whether this goes beyond the C2 center's intentions. The component will in that sense keep track of replies and related posts to the alert semantically, and will hold a status network corresponding to the process. When identified as dangerous, the component will alert a controller to initiate a calibration process, potentially a new announcement and feedback on the original alert

6.5.1.4 Alert Messages Modeling

Related functionality

Enabling automated modeling of the alerts to be generated based upon varying parameters (receiver, type of message, device capabilities, etc), so as to automatically determine best suitable format and context presentation

Description

The enabler will be able to deliver the following functionalities and characteristics:

- Categorization of different types of alerts for all potential applications
- Alert details: Specific information about the alert, the system that generated the alert and the location on a map
- Operator notes interface: Note page enables operators to capture observations associated with the alert

Features/ Supported Functionalities

The enabler is going to be composed of the following components, each delivering a respective functionality as presented below:

Component	**Functionality**
Categorization	The Categorization component will deliver the ability to distinguish the final alerts with respect to their receivers. In that sense, the Categorization component in this enabler will not care for defining priorities but only internal routing, i.e. redirecting the alerts to the respective enablers. The component will be aware of pre-defined message formats and how these are aligned to the different sensors and respective output, so as to interpret the alert fired in terms of its source, so as to define its respective recipients. Databases holding lists of interested parties (PS authorities and/or citizens) could be part of this operation and according definitions of the final user devices
User Interfaces	This component will allow the manual annotations of data and alerts, enriched with additional notes regarding the data being transmitted, especially when e.g. the recipient is another PS organization
Message Transform	The component, being aware of the available channels and the message information to be transmitted will specify how the messages should be transformed in order to be processed by the respective nodes. In this sense, the component should cover basic M2M capabilities

6.5.1.5 *Alert Communication Channel on site*

Related functionality

Awareness and management of available sensor resources to act as alerting nodes

Description

The enabler will be able to deliver the following functionalities and characteristics:

- For each of CCTV cameras deployed in the city, a speaker should also be placed in order to advice citizens in that area about some specific incident or event.

- A return communication channel can connect citizens directly with the nearest police Centre just in case citizens realize about an incident or they feel the necessity to contact with police.

Features/ Supported Functionalities

The enabler is going to be composed of the following components, each delivering a respective functionality as presented below:

Component	Functionality
Resources Awareness and Management	The component will be aware and thus continuously updated with the resources available on site for sending and receiving messages. The component should in that sense also alert when malfunctions in these resources are detected. Based on the alerts defined and triggered, the component will sent the necessary commands to the respective nodes, specifing their destination and the frequency of the alerts.
User Inputs	The component will deliver capabilities for receiving input information to be forwarded to the C2 controllers. User inputs will be standarized in order to allow automated processing and instant validation of false alarms.
Security & Network Control	The component will be responsible for securily forwarding the final message to be delivered to the output channels, taking care of QoS and security concerns.

6.5.1.6 *Traffic Light Management*

Related Functionality

<u>Automatic reconfiguration of traffic lights infrastructures to serve as public alerts</u>

Description

The enabler will be able to deliver the following functionalities and characteristics:

- Advanced reconfiguration of traffic lighting system after an incident

This expands to include

- Chaning the frequency and signaling of traffic lights, from regular to increased cautious situations
- Enabling the announcement of on-the-road messages, directly informing drivers of dangers up ahead

Features/ Supported Functionalities

The enabler is going to be composed of the following components, each delivering a respective functionality as presented below:

Component	**Functionality**
Triggering	The component will make sure that the case where a traffic light management is required is triggered. This will be done by either receiving automatic notifications by the Traffic Violation Detection enabler or manual annotations from a controller. The component will be responsible to prioritize, categorize and accordingly set an agenda for acting upon the detected cases.
Interpreting	The Triggering component will forward each case to a seperate location within the enabler's infrastructure, based on the source of the message and initial categorization criteria. From there, high-level semantics, as well as old cases will be used to trigger the according events and alerts. The component will also allow manual involvement to control the final delivery.
Responding	The Responding component will receive the final notifications to be fired and will interpret them into the according format for enabling the control of the respective devices (road-boards, traffic lights, etc). Additionally, the component will be responsible for the final delivery of the alert, making sure that the necessary connection channels and priorities have been established.

7. Summary of Generic Enablers

Table 11 below presents an overall summary of the GE enablers found being necessary in the development of the Public Safety Use Case. A briefer description upon the application of each one of the following can be found in the SafeCity deliverable D3.1 [2] while future updates of the current document are also expected to deliver more low-level details.

FIWARE reference	Name	SafeCity – Situational Awareness, Ad-hoc, Alerting, C2
3.2.1	IaaS DataCenter Resource Management	Situational Awareness, Command Centers
3.2.2	IaaS Service Management	Situational Awareness, Command Centers
3.2.3	PaaS Management	Situational Awareness
3.2.4	Object Storage	Situational Awareness
3.2.5	Cloud Edge	Situational Awareness, Command Centers
3.2.6	Monitoring	Situational Awareness, Command Centers
3.2.7	Resource Metering and Accounting	Situational Awareness
4.2.1	Big Data Processing	Situational Awareness , Ad-hoc, Command Centers
4.2.1	Publish/Subscribe Broker	Situational Awareness,
4.2.2	Complex Event Processing	Situational Awareness, Ad-hoc, Command Centers
4.2.3	Multimedia analysis to gather multimedia meta-data	Situational Awareness, Ad-hoc, Command Centers
4.2.3	Big Data Analysis	Situational Awareness, Command Centers
4.2.4	Multimedia analysis	Situational Awareness, Command Centers
4.2.4	Pre-processing of meta-data during/after gathering	Situational Awareness, Ad-hoc, Command Centers
4.2.5	Preprocessing of unstructured data	Situational Awareness, Ad-hoc
4.2.6	Meta-data Pre-processing	Situational Awareness
4.2.6	Localisation Platform	Situational Awareness, Ad-hoc, Command Centers
4.2.7	Query-access	Situational Awareness, Ad-hoc, Command Centers
4.2.8	Publish/Subscribe Broker	Situational Awareness, Ad-hoc, Command Centers
4.2.9	Semantic Annotation enabler	Situational Awareness, Ad-hoc, Command Centers
4.2.10	Semantic Application Support enabler	Situational Awareness, Ad-hoc, Command Centers
4.3.1	Social Network Analysis	Situational Awareness, Command Centers
4.3.2	Mobility Analysis	Situational Awareness, Ad-hoc, Command Centers
4.3.3	Real-time recommendations	Ad-hoc

4.3.4	Behavioural and Web profiling	Command Centers
4.3.5	Opinion mining	Command Centers
5.2.2	USDL Service Descriptions	Situational Awareness
5.2.3	Model Repository	Situational Awareness
5.2.4	Service Registry	Command Centers
5.2.8	SLA Management	Situational Awareness
5.3.3	Composition editor	Situational Awareness
5.3.4	Application mashup editor	Situational Awareness
5.3.5	Service composition	Situational Awareness
5.3.6	Execution engine	Situational Awareness
5.3.7	Mashup execution engine	Situational Awareness
5.3.8	Service composition engine	Situational Awareness
5.3.9	Service orchestration engine	Situational Awareness
5.3.10	Aggregator repository	Situational Awareness
5.4.1	Data Mediation	Situational Awareness
5.4.2	Protocol Mediation	Situational Awareness
5.4.3	Process Mediation	Situational Awareness
5.5.1	Multi-channel/Multi-device Access System	Situational Awareness
6.2.1	IoT Communications	Situational Awareness, Ad-hoc
6.2.2	IoT Resources Management	Situational Awareness, Ad-hoc
6.2.3	IoT Data handling	Situational Awareness, Ad-hoc
6.2.4	IoT Process Automation	Situational Awareness, Ad-hoc
7.2.1	Connected Devices Interfacing (CDI)	Situational Awareness, Ad-hoc
7.2.2	Cloud Edge	Situational Awareness, Ad-hoc
7.2.3	Network Information and Control (NetIC)	Situational Awareness, Ad-hoc
7.2.4	Service, Capability, Connectivity, and Control (S3C)	Situational Awareness, Ad-hoc
7.3.1	Identity and privacy management	Situational Awareness
8.2.1	Security monitoring	Situational Awareness, Ad-hoc
8.2.2	Identity Management	Situational Awareness, Ad-hoc
8.2.3	PrimeLife Policy Language (PPL) Engine	Situational Awareness

8.2.4	Identity Mixer (IdeMix)	Situational Awareness
8.2.5	Context-based security and compliance	Situational Awareness
8.2.6	Optional Security Service Enabler	Situational Awareness

Table 11 Summary of GEs required to deliver Public Safety UC's requirements

8. Summary of Specific enablers

8.1 Situational Awareness

8.1.1 Semantic Gateway

Field	Value
Source id	SAFECITY_ARA, SAFECITY_HIB
SafeCity Reference	SAFECITY_SA_1.1
Description	Handling heterogeneous sensors, filtering data upon severity and managing traffic upon sensor inputs and UC priorities
UC priority	SHOULD/ COULD
Estimate	XL
Chapter Id	FIWARE_CH4

8.1.2 Service Availability Estimation

Field	Value
Source id	SAFECITY_FOI
SafeCity Reference	SAFECITY_SA_1.2
Description	Bandwidth estimation, QoS Support, resources management and bandwidth control
UC priority	SHOULD/ COULD
Estimate	XL
Chapter Id	FIWARE_CH5

8.1.3 Semantic Definitions of Suspicious Patterns

Field	Value
Source id	SAFECITY_HIB
SafeCity Reference	SAFECITY_SA_1.3
Description	Handling of heterogeneous information and sources, delivering abilities for advanced C2 center operations (search, relate, etc)
UC priority	MUST
Estimate	XXL
Chapter Id	FIWARE_CH4

8.1.4 Suspicious Objects Detection

Field	Value
Source id	SAFECITY_ATH, SAFECITY_AIT
SafeCity Reference	SAFECITY_SA_1.4
Description	Automatic detection of threats concerned with orphan objects, contained weapons, etc
UC priority	MUST
Estimate	L
Chapter Id	FIWARE_CH4

8.1.5 Suspicious Citizen Behavior Detection

Field	Value
Source id	SAFECITY_ATH, SAFECITY_AIT, SAFECITY_THA
SafeCity Reference	SAFECITY_SA_1.5
Description	Automatic detection and prediction of threats concerned with suspicious citizens
UC priority	MUST
Estimate	L
Chapter Id	FIWARE_CH4

8.1.6 Detection of Violation to Restricted Areas

Field	Value
Source id	SAFECITY_ATH, SAFECITY_AIT
SafeCity Reference	SAFECITY_SA_1.6
Description	Automatic detection and prediction of threats concerned with unauthorized access
UC priority	MUST
Estimate	L
Chapter Id	FIWARE_CH4

8.1.7 Detection & Identification

Field	Value
Source id	SAFECITY_ATH, SAFECITY_AIT
SafeCity Reference	SAFECITY_SA_1.7
Description	Specific features recognition (citizens and objects), identificationof specific patterns across a crowd

UC priority	MUST/ SHOULD
Estimate	XXL
Chapter Id	FIWARE_CH4

8.1.8 Real-time Positioning and Tracking

Field	Value
Source id	SAFECITY_THA
SafeCity Reference	SAFECITY_SA_1.8
Description	Position awareness and tracking capabilities upon given patterns, across neighborhood sensors
UC priority	MUST/ SHOULD
Estimate	XXL
Chapter Id	FIWARE_CH4

8.1.9 Traffic Violation Detection

Field	Value
Source id	SAFECITY_VTT
SafeCity Reference	SAFECITY_SA_1.9
Description	Automatic detection of threats related to traffic behavior
UC priority	MUST
Estimate	XL
Chapter Id	FIWARE_CH4

8.1.10 Environmental incident detection

Field	Value
Source id	SAFECITY_VTT
SafeCity Reference	SAFECITY_SA_1.10
Description	Automatic detection and prediction of threats triggered by environmental indicators (fire, bio-chemical attacks, etc)
UC priority	MUST
Estimate	XL
Chapter Id	FIWARE_CH4

8.1.11 Cold Vehicles

Field	Value

Source id	SAFECITY_FOI
SafeCity Reference	SAFECITY_SA_1.11
Description	Definition of risk of cold behicles in a traffic jam on a certain road section using information from temperature, infra-red and video sensors, as well as statistical prediction models
UC priority	MUST
Estimate	XL
Chapter Id	FIWARE_CH4

8.1.12 Real-Time Masking

Field	Value
Source id	SAFECITY_ARA
SafeCity Reference	SAFECITY_SA_1.12
Description	Automatic data filtering being in compliance with citizens' privacy regulations
UC priority	MUST
Estimate	XL
Chapter Id	FIWARE_CH4

8.1.13 Personnal Data Destruction

Field	Value
Source id	SAFECITY_ARA
SafeCity Reference	SAFECITY_SA_1.13
Description	Absolute and permanent destruction of the personnal data collected, once these exceed their maximum allowed temporal availability
UC priority	MUST
Estimate	XL
Chapter Id	FIWARE_CH4

8.2 Ad-hoc Networks

8.2.1 Wireless Sensors Networks

Field	Value
Source id	SAFECITY_TEK
SafeCity Reference	SAFECITY_ADHOC_1.1
Description	An enabler to introduce the ability to include wireless communication among channels, so as to favor a city-wide coverage
UC priority	MUST
Estimate	XL
Chapter Id	FIWARE_CH7

8.2.2 Support for airborne communication relay platforms

Field	Value
Source id	SAFECITY_FOI
SafeCity Reference	SAFECITY_ADHOC_1.2
Description	Automatic network support for heterogeneous networks
UC priority	MUST
Estimate	XL
Chapter Id	FIWARE_CH7

8.2.3 Mobile Command Centers Connection

Field	Value
Source id	SAFECITY_TEK
SafeCity Reference	SAFECITY_ADHOC_1.3
Description	An enabler to introduce the ability to maintain communication with mobile C2 in the area at all times
UC priority	MUST
Estimate	XL
Chapter Id	FIWARE_CH7

8.2.4 Communication with Police Units while on the move

Field	Value
Source id	SAFECITY_TEK
SafeCity Reference	SAFECITY_ADHOC_1.4

Description	An enabler to introduce the ability to maintain communication across mobile patrols in the area and the main C2 centre at all times
UC priority	MUST
Estimate	XL
Chapter Id	FIWARE_CH7

8.3 Command Centers

8.3.1 Incident Detection Indicator

Field	Value
Source id	SAFECITY_MIT
SafeCity Reference	SAFECITY_C2_1.1
Description	Automatic (i.e. including minimum human intervention) identification of alarms (detection of an alarm and recognition of its nature), threat validation
UC priority	MUST/ SHOULD
Estimate	L
Chapter Id	FIWARE_CH4
VidChapter Id	FIWARE_CH4

8.3.2 Common Operating Picture (COP)

Field	Value
Source id	SAFECITY_MIT
SafeCity Reference	SAFECITY_C2_1.2
Description	Advanced interactive user interface for online and offline holitic data analysis
UC priority	MUST/SHOULD
Estimate	XXL
Chapter Id	FIWARE_CH4

8.3.3 Public Spaces Visualization

Field	Value
Source id	SAFECITY_MIT
SafeCity Reference	SAFECITY_C2_1.3
Description	Ability to acquire inputs from CCTV cameras towards creating life-like simulations of the area being monitoring (3D representation on buildings and persons, clear reference on street names, etc)
UC priority	MUST
Estimate	XXL

Chapter Id	FIWARE_CH4

8.3.4 Management of Video Stored Information

Field	Value
Source id	SAFECITY_THA
SafeCity Reference	SAFECITY_C2_1.4
Description	Processing capabilities dealing with data storage and retrieval efficiency for effective handling of vast amount of demanding data
UC priority	MUST
Estimate	XL
Chapter Id	FIWARE_CH4

8.3.5 Unified Incident Management (Public Safety Resources)

Field	Value
Source id	SAFECITY_ISD
SafeCity Reference	SAFECITY_C2_1.5
Description	Awareness of available resources and coordination interface among PS authorities
UC priority	MUST/SHOULD
Estimate	XXL
Chapter Id	FIWARE_CH4, FIWARE_CH6, FIWARE_CH7

8.4 Alerting technologies

8.4.1 Alert Activation through fix telephone networks

Field	Value
Source id	SAFECITY_
SafeCity Reference	SAFECITY_ALERT_1.1
Description	Enabling the automatic transmission of alerts through landline infrastructures
UC priority	MUST
Estimate	S
Chapter Id	FIWARE_CH7

8.4.2 Alert Activation through Mobile Phones

Field	Value
Source id	SAFECITY_TIL
SafeCity Reference	SAFECITY_ALERT_1.2
Description	Enabling the automatic transmission of alerts through cellular telephony networks (e.g. in the form of text message - SMS)
UC priority	MUST
Estimate	S
Chapter Id	FIWARE_CH7

8.4.3 Alert Activation through Internet Networks

Field	Value
Source id	SAFECITY_HIB
SafeCity Reference	SAFECITY_ALERT_1.3
Description	Viral alerting of citizens and PS authorities through online social networks (offers global coverage and full time support)
UC priority	MUST
Estimate	S
Chapter Id	FIWARE_CH7

8.4.4 Alert Messages Modeling

Field	Value
Source id	SAFECITY_MIT
SafeCity Reference	SAFECITY_ALERT_1.4

Description	Enabling automated modeling of the alerts to be generated based upon varying parameters (receiver, type of message, device capabilities, etc), so as to automatically determine best suitable format and context presentation
UC priority	SHOULD/COULD
Estimate	L
Chapter Id	FIWARE_CH4

8.4.5 Alert Communication Channel on site

Field	**Value**
Source id	SAFECITY_TEK
SafeCity Reference	SAFECITY_ALERT_1.5
Description	Awareness and management of available sensor resources to act as alerting nodes
UC priority	MUST
Estimate	L
Chapter Id	FIWARE_CH7/ FIWARE_CH6

8.4.6 Traffic Light Management

Field	**Value**
Source id	SAFECITY_VTT
SafeCity Reference	SAFECITY_ALERT_1.6
Description	Automatic reconfiguration of traffic lights infrastructures to serve as public alerts
UC priority	MUST
Estimate	L
Chapter Id	FIWARE_CH4