FP7-285556 SafeCity Project

Deliverable D3.1

Title: Specific Requirements Definition

Deliverable Type:	**CO**
Nature of the Deliverable:	**R**
Date:	**25/10/2011**
Distribution:	**WP3**
Editors:	**THALES**
Contributors:	**WP3 partners ie. ISD, AIT, ARA, TEK, ATH, HIB, MIT, TIS, VTT, FOI, 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 requirements 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 endeavoured to achieve the degree of accuracy and reliability appropriate to the work in question. However since the partners have no control over the use to which the information contained within the report is to be put by any other party, any other such party shall be deemed to have satisfied itself as to the suitability and reliability of the information in relation to any particular use, purpose or application.

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

List of Authors

Partner	Authors
THALES	Sophie Chagué, Johan D'hose, Fabien Flacher, Rhalem Zouaoui
HI-IBERIA	Roberto Giménez, Emilio Martín, Diego Fuentes
AIT	Tassos Dimitriou, Sofia Tsekeridou
ARA	Myrto Zacharaki, Giorgos Kostopoulos
ATH	Peretz Gurel
MIT	Lucian Adrei
VTT	Sami Ruponen, Timo Kyntäjä
TEK	Pedro Antonio
TIS	Roberto Gavazzi

Document History

Date	Version	Editor	Change	Status
20110701	0	THA Sophie Chagué	First Draft of SafeCity deliverable template	Draft
	0.1	THA Johan D'hose	Review	Draft
20110822	0.2	THA Sophie Chagué Rhalem Zouaoui	§2.4 completion	Draft
20110831	0.3	THA Sophie Chagué	MIT+HIB +AIT : contributions integration	Draft
20110907	0.5	THA Sophie Chagué	VTT+TEK+ATH+ARA : contributions integration	Draft
20110927	0.6	THA Sophie Chagué	Contribution Updates	Draft
20110930	0.7	THA Sophie Chagué	TIL+AIT : Contribution Updates	Draft
20111006	0.8	THA Sophie Chagué	MIT+VTT+ATH/AIT : Contribution Updates	Draft
20111010	0.9	THA Sophie Chagué	HIB : slight presentation updates THA: correction of the overall document	Draft
20111014	1	THA Sophie Chagué	AIT+THA +TIS+VTT+HIB corrections integration	Draft
20111025	1.1	THA Sophie Chagué	Corrections from HIB review of the deliverable + TEK updates	Draft
20111028	2	ISD Judith Pertejo	Reviewed deliverable	Draft M6

Table of Contents

List of Figures

List of Tables

Glossary

Acronym	Meaning
AI	Artificial Intelligence
ARA	Aratos Technologies
ATH	Athena
C2	Command Center
DSS	Decision Support System
FOL	First Order Logic
GE	Generic Enabler
HIB	HI-IBERIA
MIT	Mira Telecom
N/A	Not Applicable
SE	Specific Enabler
SC	Security Configuration
THALES	Thales
TEK	Tekever
TIS	Telecom Italia
UI	User Interface

References

Number	Reference
[1]	FI-WARE High Level Description (Product Vision), Fi-WARE-11-08-1
[2]	Backlog entries description.xls
[3]	SafeCity report D2.8 Specific Enablers on Public Safety in Smart CIties

1. Introduction

The main objective of the task T3.1 is to identify the architectural requirements to be developed through the Core Platform in order to capacitate it to provide the Public Safety smart capabilities.

This work will complete the functional analysis (top down approach) and enablers definition realized in D2.8. Indeed, D2.8 focuses on the analysis of the Public Safety Use cases and establishes the functional requirements of the SafeCity system. It also describes – work in progress - the capabilities of the enablers required in response to them.

In parallel, based on a bottom up approach, work in progress in D3.1 aims to identify for each WP4 applications[1], Public Safety features and **technical requirements**. In order to achieve this task, in line with the overall FI-PPP program planning and organization, we will also put a particular attention to the High Level Description Document provided by FI-WARE in order to identify proposed features in [1] that SafeCity WP4 applications will need.

This work will prepare our **features backlog** [2] that we will deliver to FI-WARE.

In following versions of the document, we plan to generalize this approach for each Public Safety scenarios, in order to gather in a more global approach technical requirements.

[1] WP4 applications are the following : Application 1 “generating Situation Insights based on Video Analytics”, Application 2 “Ad-Hoc Networks”, Application 3 “Intelligent Sensors and Information Pre-Processing”, Application 4 “Real-time Positioning based on Video Analysis and Artificial Intelligence for Decision Support, Application 5 “Data Fusion”, Application 6 “Information Security”, Application 7 “Decision Support”, Application 8 “Road track and environmental sensors”.

2. Application 1 "Generating situation Insight based on Video Analytics" Features and Requirements

2.1 Short description

The Video Analytics application, jointly contributed by AIT and ATHENA, is primarily aimed for C2 centres to support decision making and alerting of C2 personnel in case of emergency (accident, disaster, etc.) and/or threatening situations (suspicious acts that may lead to crime, terrorism, etc.) by analyzing video feeds from surveillance digital cameras positioned in a city and visually detecting potential life or property threatening situations.

In order to achieve that, Application 1 will fully specify a semantic-based video analytics engine operated at the Command Centre using available city-wide video surveillance systems for situational awareness and alerting. More specifically, it will proceed by:

- Defining a number of suspicious or threatening situations indicating suspicious behavior or actions that (may) lead to threat to human lives, property, etc.
- Formally representing such implicit domain knowledge (using ontologies) and defining the reasoning rules and algorithms for understanding such situations based on what is visually perceived and detected by the video analysis process
- Analyzing video data (stored and streamed) to extract useful insights and hints about occurrences in monitored city areas that relate to the defined safety situations
- Alerting C2 personnel when such potential situations may emerge to take the necessary action and/or informing other SafeCity applications (such as Data Fusion and/or Decision Support System) to support their automated decisions and improve their accuracy

Achievements

AIT and ATHENA's Video Analytics Application will offer functionalities such as:

- increase the visual monitoring efficiency in Command Centers by largely automating visual monitoring and detection of suspicious incidents. It is a usual case that thousands of surveillance cameras are installed in areas desired to be monitored (e.g. cities) while only tens of operators are available to view the feeds of the cameras and manually detect any potential threat. Thus, it will further contribute to the reduction of the significant information load of C2 personnel
- generate immediate alerts for potential suspicious happenings, visually detected, and/or feed into with situation insights and thus enhance the efficiency of the Data Fusion and Decision Support System Enablers of SafeCity. At the long run, better situational awareness will be accomplished and more immediate human action will be triggered.
- in certain cases, detect the pre-conditions of a potentially evolving dangerous situation and thus allow C2 personnel to act proactively and limit the progression of it or even anticipate and prevent a dangerous situation

2.2 Features identification

The conceptually defined Semantic-based Video Analytics Engine (Application 1) targeted to the generation of potentially threatening or suspicious situation insights, in order to achieve its objectives, necessitates the inclusion of the following two fundamental major components, each one with a required set of sub-components that could be characterized as either generic or SafeCity specific enablers:

- **Data Modeling and Handling, Knowledge Representation and Reasoning in the Safety and Security Domain**, including the following data assets and functionalities/sub-components:
    - *Knowledge Representation and Data Modeling*: Safety and security-related knowledge models (domain and multimedia ontologies), taxonomies and respective data models will be introduced (up to Phase 2), for data interoperability among the SafeCity applications and in order to facilitate automated reasoning and inferencing on top of detected primitive events, objects, etc. during video analysis towards efficiently identifying emergency events or suspicious behaviours. These knowledge and data models will allow for spatial and/or time-based co-occurrences of detected spatio-temporal patterns (e.g. movement), objects or event primitives in video data that are in line with the "rules" dictated in the defined ontologies.
    - *Data/Metadata Handling*: appropriate editor as well as parsing tools are necessary for creating/updating the above mentioned knowledge models and metadata schemas, such as Protégé for ontologies or the Xerces XML parser for XML-based metadata, as well as for encoding/decoding, playing back and streaming video data.
    - *Data/Metadata Storage*: furthermore, with respect to their storage, video data and metadata are expected to be stored in the generic SafeCity C2 respective archive while Data models, Ontologies, Rules, etc. compose the generic SafeCity knowledge repository (as depicted in Figure 1 and Figure 2).
    - *Reasoning Engine* (shown in Figure 2) that includes inference algorithms based on e.g. description logics or FOL and operates on top of the defined SafeCity Ontologies and associated rules in order to infer higher level semantics with respect to situation insights. Reasoning is focused mainly on how to assess the spatiotemporal sequence of a variety of detected objects and event primitives in the video stream into a semantically defined suspicious behaviour instance, existent in the SafeCity safety ontology.
    - *Metadata generation and parsing* component, that allows the automatic generation of metadata instances following the adopted metadata schemas, carrying semantic, structural, operational and low-level information on visually processed data and the situation insights produced. It is further required that the ability to search among metadata and parse them is provided e. g. for the case of retrieving past data from the SafeCity data archive, or in case that other SafeCity applications are parsing the metadata information such as the Data Fusion or Decision Support System applications (data interoperability of data exchanges among diverse SafeCity applications).

- *Ontology Evolution* component (shown in Figure 2) that updates ontological definitions and associated inference rules based on new findings (assisted also by the Data Fusion and DSS systems) as well as C2 personnel observations (through interactions) in dynamic video data with respect e.g. to new behavioral patterns or limited efficiency of the initial ontology to capture a specific event instance.

- **Video analytics Engine;** the functionalities/sub-components of this component are the following:

  - *Video Processing and Analysis Engine* including a rich set of automated or semi-automated (where required) image/video processing algorithms such as:

    - Region/Object segmentation (car, person, animal, vehicle, etc.) by color, shape, texture, edges, etc.
    - Motion Estimation
    - Moving Object Segmentation
    - Moving Object Tracking (person, vehicle, animal, etc.)
    - Foreground/Background Detection
    - Face detection
    - Face identification
    - Orphan object detection
    - Car detection and tracking
    - License Plate recognition
    - Line drawing
    - Change detection
    - Activity Detection
    - Event Classification and Detection (use of the respective ontology and pattern recognition algorithms)
    - Suspicious Behaviour Classification and Detection (use of the respective ontology and pattern recognition algorithms) such as detection of loitering, fights, races, falls, movement against the flow of traffic, etc.

    A sub-component of the engine further performs *video pre-processing for video content filtering* and selective video data streaming at the ARATOS gateway, which ideally is performed in real-time at low processing and memory capabilities hardware. The tasks performed include the following:

    - Noise filtering
    - Illumination changes compensation

- Activity detection
- Change detection

In many cases, the type and sequence of the video processing and analysis steps is driven by the predefined safety and security related knowledge domain representations to lead to the desired situation insights generation.

- *Visual descriptors extraction* component. It extracts, through video analysis and feature extraction algorithms, visual descriptors from previously segmented spatial, temporal or spatio-temporal regions. The purpose is to efficiently describe visual primitives from video data with low-level visual metadata that will further serve as input to either the pattern recognition modeling phase (during training assuming that the required amount of training video data is available) or the detection/matching phase.

- *Pattern Recognition algorithms.* Both classification (SVM, LVQ, etc.) and clustering (density-based, etc.) algorithms will formulate a pattern recognition engine that will be used, having as input visual feature vectors (single or combined), to either produce object, behaviour or primitive event models during the training phase of supervised learning algorithms using training video data from prior threatening events (Figure 1), or generate clusters of such entities using video data from prior threatening events for which respective a priori knowledge does not exist (Figure 1), or detect and identify during the testing phase of both classification or clustering algorithms the situation hint (object, primitive event or behaviour) during the overall process of situation insights generation. The modeling phase generates behavioural models and detected patterns in visual data from previous similar public safety threat events in archived video feeds, while the detection phase is assisted by them to identify the exact detected object or primitive event/behaviour in the currently monitored video feed.

- *Model retraining* component (Figure 2). It is often the case that learned models in classification algorithms or clusters in clustering algorithms, due to insufficiency of training data or noisy data, are often not optimal or fail to represent the full potential of a specific concept or entity. With the provision of new video data through the constant monitoring process, these serve as input for model retraining (running the classification and clustering algorithms to reproduce models or clusters) in case that this process leads to higher accuracy of the latter. Furthermore, the validation of detection results by human operators at the Command Centre facilitates this process even more and with a higher accuracy. Both these tasks are considered in a component dealing with model retraining

Application 1: Video Analytics requires an offline preparation phase in order to optimally perform in a (near) real-time operational setting. Thus, Figure 1 presents the necessary architectural components (as presented above) of the offline data assets creation and video processing operational system that essentially generates all the necessary data that are needed during the (near) real-time operation of the Semantic-based Video Analytics Engine.

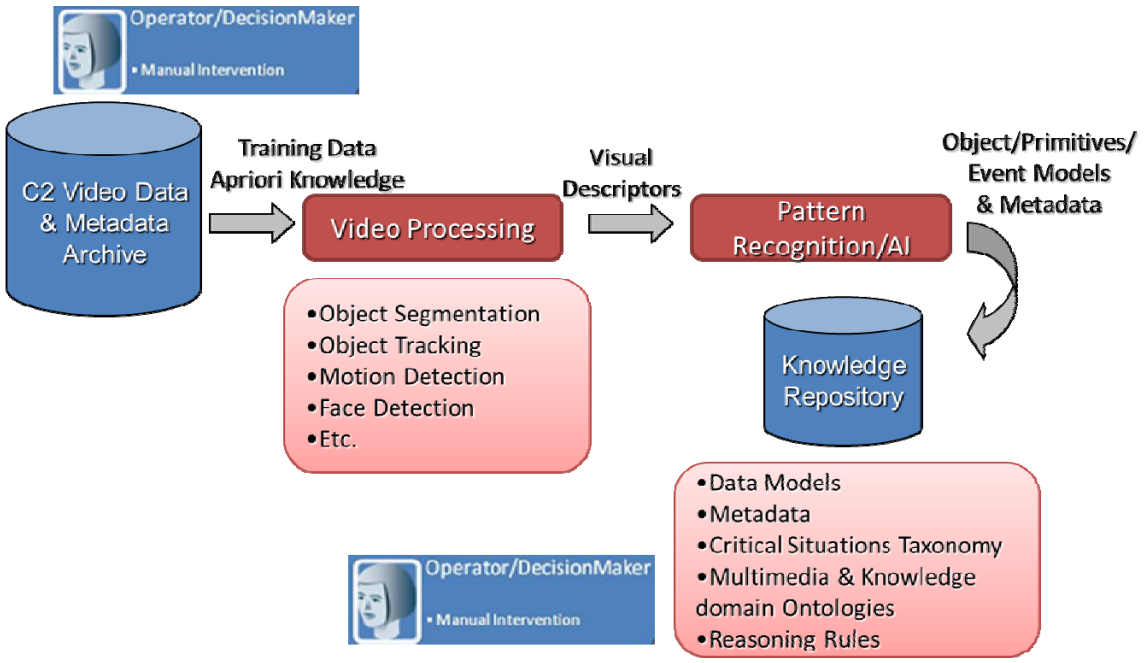


Figure 1 Offline Data Creation and Video Processing sub-system of the Video Analytics Application

Complementary, Figure 2 illustrates the necessary architectural components (as presented above) of the (near) real-time semantic-based video analytics operational system that produces situation insights communicated either directly to the C2 personnel or/and outputted to the Data Fusion and DSS systems of SafeCity.

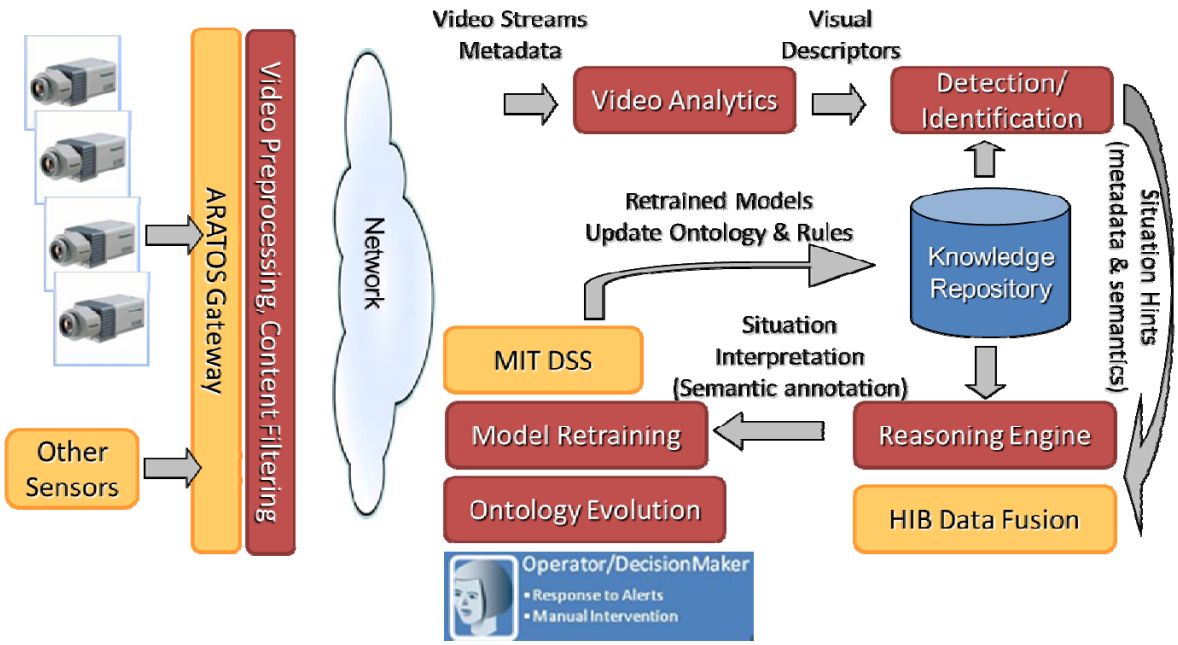


Figure 2 (Near) Real-time Semantic-based Video Analytics Application reasoning out situation insights

In order to demonstrate the added value and efficiency of Application 1, we have defined below an initial set of threat scenarios for which Application 1 will fully define a functional system for their efficient detection, thus providing relevant insights to C2 personnel and the SafeCity Data Fusion and DSS applications. Each one of the defined scenarios requires a subset of the components/enablers mentioned above. It is noted that this list will be extended to include other scenarios based on user needs and other defined situations that need to be handled by Application 1 and that will be formally represented in the respective SafeCity ontology. In Figures 1 and 2 the blue components are generic SafeCity components (Data Archive, Knowledge Repository), the orange components present other SafeCity Applications with which Application 1 – Video Analytics interfaces and communicates, while the reddish components are Application 1 specific components.

Scenario 1: Suspicious people

Operational Settings:

A CCTV camera is installed at an entry to a building.

The video stream from the camera is connected to a nearby gateway[2], located at a secure area. There it is recorded. A copy of the recording is kept for evaluation of the system operation.

Functional Description:

The video analysis software running on the gateway is constantly coarsely searching for a face region (coarse face detection function based on color information) – optimal face detection is feasible even in semi-frontal views based on color and shape descriptors as well as the biometrics of the face region but face recognition is optimally performed only in frontal views. This poses a constraint for this type of processing. Whenever a face region is coarsely detected in the incoming video stream the software either captures a short (several seconds) video clip with the face region in it or starts streaming the video feed to the C2 center over secure communication channel for a short duration.

In the C2 center the Video analytics Engine further processes the coarsely detected face region to deduce with higher accuracy the face region (if correctly detected initially) and extracts unique visual features/descriptors (according to the method of face identity modeling to be used). Subsequently it compares the detected facial features to a database of known face models of "bad persons" (face recognition function) – these models have been generated from existing video training data beforehand, in an offline mode, using video processing and pattern recognition algorithms and the same set of visual features to characterize face regions. If a match is found, the component raises an alarm, indicating the suspicious face region and detected identity, and forwards this information (metadata instance) to the Data Fusion and DSS applications. The operator verifies the accuracy of the results and, if so, the system is capable to use the new video data of the identified face to optimize the trained models and algorithms for face identification.

Required components/enablers:

- Knowledge Representation and Data Modeling: Metadata schema definition

[2] It is assumed that the Gateway (any instance of a gateway mentioned in the scenarios) will have the required processing power, storage space, operation system and other basic software components (exact requirements are to be defined).

- Data/Metadata Handling: metadata parsing, video data encoding/decoding, streaming and playback
- Data/Metadata Storage: archiving captured video feeds and metadata instances
- Video Processing and Analysis Engine: color segmentation and coarse face region detection at gateway, color/shape segmentation and biometrics estimation for optimal face detection, face identification
- Visual descriptors extraction: color and shape features, biometrics from detected face regions
- Pattern recognition: face identity models generation (training phase), face identity detection (matching phase)_
- Metadata generation: carrying results of detection and identification stages (e.g. face region, face identity, time stamp)
- Model retraining (if needed)

Scenario 2: Orphan objects

Operational Settings:

A CCTV camera is installed in a street.

The video stream from the camera is connected to a nearby gateway, located at a secure area. There it is recorded. A copy of the recording is kept for evaluation of the system operation.

Functional Description:

The video analysis software running on the gateway is first calibrated to an empty space to register the background non-moving information (buildings, trees, etc.). From that moment onwards, it starts detecting changes in motion and activity. If changes are detected, it starts streaming the video feed to the C2 center over secure communication channel. There, the video analytics engine processes motion information and detects moving objects, attempting to identify, particularly, people passing b, by analyzing the scene/object motion and monitoring their continuity. The incidence of a moving object that remains in the scene but stops moving for a significant duration of time, i.e. the appearance of a new static object (could be a bag, box, suitcase, stroller, etc.) initiates a potential alert and is associated with the last passerby that walked through that same spot. The video analytics software will start a timer and if it goes off before someone takes away the bag, the software raises an alarm to a C2 personnel to check the threatening potential of the situation, indicating the suspicious object and associated passerby, and forwards this information (metadata instance) to the Data Fusion and DSS applications.

Required components/enablers:

- Knowledge Representation and Data Modeling: Metadata schema definition
- Data/Metadata Handling: metadata parsing, video data encoding/decoding, streaming and playback
- Data/Metadata Storage: archiving captured video feeds and metadata instances
- Video Processing and Analysis Engine: background registration, change detection, motion estimation, activity detection, moving object segmentation, moving object tracking, person detection, person tracking, orphan object detection
- Metadata generation: carrying results of detection and identification stages (e.g. object region, location, associated person region, time stamp)

Scenario 3 Entry into a secure area

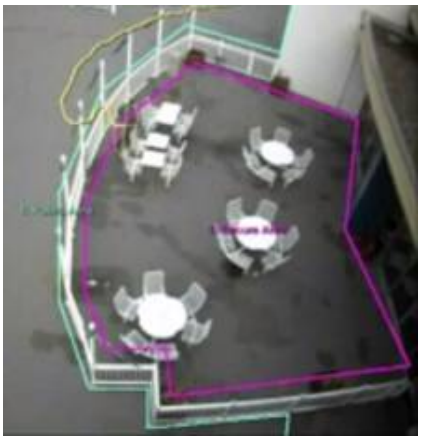
Operational Settings:

A CCTV camera, mounted several meters above the ground, is looking down at a scene. The scene includes a secure area (described by a purple polygon in the picture below).

The video stream from the camera is connected to a nearby gateway. There it is recorded. A copy of the recording is kept for evaluation of the system operation.

Functional Description:

The video analysis software running on the gateway is constantly searching for motion/activity at the region near the secure area. If this is the case, it starts streaming the video feed to the C2 center over secure communication channel. There, the video analytics engine processes the motion information looking for potential transition of persons/objects into the secure area. Whenever such an activity takes place, an alert is sent to the secured C2 center indicating the area of intrusion and the intruding person/object, and forwards this information (metadata instance) to the Data Fusion and DSS applications.



Required components/enablers:

- Knowledge Representation and Data Modeling: Metadata schema definition
- Data/Metadata Handling: metadata parsing, video data encoding/decoding, streaming and playback
- Data/Metadata Storage: archiving captured video feeds and metadata instances
- Video Processing and Analysis Engine: secure area determination (virtual line drawing, manually determined), region-based change/activity detection, motion estimation, moving object segmentation, moving object tracking, trespassing detection
- Metadata generation: carrying results of detection and identification stages (e.g. location of trespassing, associated region, time stamp)

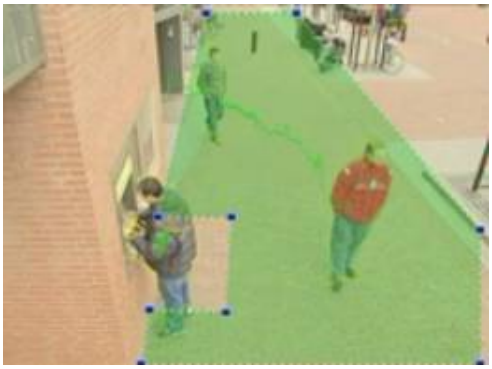
Scenario 4: Suspicious behavior

Operational Settings:

A CCTV camera is installed at a height of about 4 meters, looking down on the street.

The video stream from the camera is connected to a nearby gateway, located at a secure area. There it is recorded. A copy of the recording is kept for evaluation of the system operation.

Functional Description:



The video analysis software running on the gateway is coarsely detecting moving regions in the nearby area. When such are detected, it starts streaming the video feed to the C2 center over secure communication channel along with the coordinates and the bounding box of the moving region. The coordinates are coupled with time stamps (metadata). There, the video analytics engine processes the information to determine whether it is a moving person

If several persons appear simultaneously in the video data, the video analysis software attempts to estimate the coordinates/timestamp information for each person separately (the feasibility and accuracy depends on the number of overlapping and occluded regions).

The C2 software will analyze the pattern of movement of each person and decide if it is “Normal” or “Suspicious”. The second case will trigger an alarm identifying the suspicious movement pattern, according to reasoning rules as defined in the SafeCity knowledge repository. An example for a suspicious person movement pattern is going back and forth for a long time near the ATM (“wandering” pattern). The scenario necessitates the a priori definition of a suspicious behaviours list and their association with visual events/objects and reasoning rules, within the SafeCity ontology.

Required components/enablers:

- Knowledge Representation and Data Modeling: Threat ontology definition including suspicious behaviours and relations with visual events/objects and motion patterns, Metadata schema definition
- Data/Metadata Handling: ontology editors, metadata parsing, video data encoding/decoding, streaming and playback
- Data/Metadata Storage: archiving captured video feeds and metadata instances
- Video Processing and Analysis Engine: region of interest determination (virtual line drawing, manually determined), background scene registration, motion estimation, moving region/object segmentation, moving object tracking, person tracking
- Metadata generation: carrying results of detection and identification stages (e.g. detected suspicious behaviour, associated region/person, time stamp)

- Reasoning Engine: to infer based on predefined rules the type of suspicious behaviour based on visual hints (e.g. motion patterns) produced by the video analytics engine and their spatio-temporal co-occurrences.

- Ontology Evolution (if needed): for the update of current suspicious behaviours and the insertion of newly defined

A preliminary architectural setup of the proof of concept trial, including all respective SafeCity applications, as part of WP4, that will be implemented in Madrid.

In this setup, it is important to note the following limitations and constraints that may affect the desired functionality of Application 1:

1. Video cameras will be installed in the Montera street in Madrid. This location was selected for the following reasons:

    a. It is possible to install the project cameras only in locations where cameras are already in use (permission was already granted for these locations). This however may affect the requirements for placement at a specific height as needed by some of the initial Scenarios (e.g. Scenario no. 3)

    b. In the Montera street IP connectivity is already available, connecting the project cameras directly – via the MCC (Madrid City Council) private secure high speed IP network – to the MCC command centre – it is to be decided where exactly the ARATOS gateway will be connected.

2. At the network edge, the video streams, along with the other placed field sensors, will be connected to a Gateway (provided by Aratos). This Gateway will quickly pre-process video streams as specified for the initial set of defined scenarios above.

3. The video streams will then be directed to the “FI-WARE private cloud services”, where the FI-WARE Generic Enablers (such as the Multimedia analysis GE and the Semantic Application Support GE) will further process the video streams, as specified in the scenarios description above. It is noted that the allocation of processing between the Gateway and the FI-WARE private cloud remains to be determined.

4. The detection and reasoning results from the Semantic-Based Video Analytics Application will be communicated to other SafeCity applications, namely:

    a. Data Fusion

    b. Decision Support System

Apart from specific cases, these applications will present potential detected alerts to human operators of the Command Center.

2.3 Requirements

Requirements	Generic Expression	Expression of requirements within the scope of the 1st WP4 trials
Video Quality requirements	In order to efficiently perform video analysis: • Image quality : 4CIF (or VGA) • Video compression: H.264 or MJPEG • 8-12 frames/sec (=>Compression rate 8 to 48)	Additionally: Scenario 1: frontal faces in captured video, minimum illumination changes (constant lighting) Scenario 2:
Bandwidth requirements	Assumptions: 100 to 8000 cameras 2Mbits/sec to 8Mbits/sec per video stream.	Assumptions : 4 cameras for the demonstration (of the 4 scenarios if feasible) 1-2Mbits/sec per stream should be sufficient
SafeCity Ontology and Multimedia Ontologies definition Requirement	To assist the process of semantics extraction and scene understanding, especially with respect to suspicious behaviour detection (Scenario 4), a Safety and security ontology needs to be defined, including the list of potential threat scenarios and the association with primitive events/objects/patterns. Respectively, multimedia and temporal ontologies need to be defined to associate semantic primitives with spatio-temporal visual ones. For the definition an ontology editor such as Protégé is needed supporting ontology languages such as OWL or OWL2	Proper definition of the "wandering" suspicious behaviour and its correspondence to spatio-temporal visual primitives (visual objects, movement patterns, vicinity, etc.)
Privacy requirements	Personal data (faces, number plates, private buildings, etc.) contained in the video must be protected from illegal access	No need for the trials, trial data to be prepared with prior information and written consent of the participating volunteers (consortium members or users).
Reasoner engine	To infer new knowledge or high level semantic information from low-level visual hints and their spatio-temporal sequences, based on the defined ontologies, a Reasoner Engine is required, such as • Racer • Pellet	Optional, if **only** the "wandering" behaviour to be tackled in Phase I (could be accommodated with properly defined reasoning rules).
Video Data, Data Models and Metadata Archive of Prior Events,	To produce data models (face identity models, object models, motion pattern models, etc.) there is a need for prior recorded video data and their associated metadata instances to be used as training content and ground truth data for the pattern recognition algorithms. Such data should reside in a video data and metadata archive along with produced models with the available interface API for easy search,	Such data are going in a large extent to be artificially constructed using e.g. volunteers to capture face videos, assign identities and train algorithms to produce face identity models, recording staged events as prior/historical video data, manually (or assisted by authoring tool) constructing necessary metadata instances, etc. Background

	querying, retrieval, updating. Furthermore, other type of data, such as background scene images, secure area perimeters (spatial coordinates and shape), etc. of the monitored areas should be stored in the archive for access in (near) real-time operation mode.	registration of monitored scenes, secure areas perimeter definition, etc. to be captured and stored in a preparation phase. Need for respective archive and interfaces availability for querying, searching updating the stored data.
Metadata Instances	An adequate metadata schema will be defined for all types of metadata: visual low-level (feature vectors), structural (spatio—temporal information in video data associated with segment of interest (object, face, moving person, etc.), configuration, semantic (these are instantiated based also on ontological definitions). Metadata instances accompanying recorded video data and including results of the analysis process should comply to this schema and be stored in the respective archive as well as forwarded to the other SafeCity Applications (Data Fusion, DSS)	Metadata instances should carry the detected results information as defined for the four Scenarios above.
Security Requirements	New connected sensor or accessing user must be authenticated before having access to the applications, devices. The access level to applications, devices and ad-hoc network must be dynamically configurable	Optional
Memory and Computational requirements	Video Analytics, especially when performed in real-time, necessitates intensive use of memory and computational resources and parallelism of processes especially when the feeds of many cameras are simultaneously processed. Similarly, real-time reasoning engines have similar requirements for inferring high level semantics and knowledge. The capability to use cloud computing and storage resources through respective enablers is necessary. .	Desirable
Network Latency, Guaranteed Service	Network latency needs to be kept to minimum levels, as well as the transport service needs to be guaranteed (no losses, no errors) so as to guarantee that the pre-processing metadata produced by coarse video processing performed at the gateway reach the C2 center on time and	Desirable.

	without errors prior to the event/situation having already evolved.	

Further specific requirements, with respect to the initial set of defined scenarios, are summarized to the following:

- Digital camera installation requirements (if possible with respect to the current camera installations at the Montera street):
    - *Scenario 1*: A single camera, installed at an entry to a building, in a position that allows a very good frontal view (in good resolution) of the faces of the people entering the building (ideally at a height of 1.60-1.80 meters).
    - *Scenario 2*: A single camera, ideally installed at a height of 2.50-3.00 meters.
    - *Scenario 3*: A single camera, installed in a high (several meters) position looking down at a secure area.
    - *Scenario 4*: A single camera, in a position that allows it a wide view of the area (ideally at a height of several meters)
- Gateway capabilities and connectivity:
    - A gateway, located at a secured area near the installed camera(s), with significant processing power and storage space for local coarse video processing, running Windows or similar OS, connected over a high bandwidth secure channel to the video analytics server at the C2 centre.
- Input/Configuration Data requirements:
    - Video data streams and metadata instances
    - Number, location, field of view, characteristics (compression, resolution, frame rate, capabilities (if any) for local processing, etc.) of installed digital cameras for both Madrid and Stockholm cities (one time insertion to the system).
    - Safety and Security-related ontologies and taxonomies in the SafeCity Knowledge Repository to drive the semantic based video analysis and reasoning out of situation insights, e.g. a threat ontology definition including suspicious behaviours and their association with visual events/objects and their spatio-temporal evolution dictated through properly defined rules
    - Training content and Ground truth data (from prior events)
        - Face models of “bad persons” installed in the C2 server in the C2 centre for face detection
        - Trained Object models

- Behaviour/Pattern Profiles and Historical data (video streams and metadata(from past events of scenarios/events to be sought for

- Algorithmic parameter inputs for video processing and pattern recognition algorithms, e.g.
  - Idle timer's value (that will raise the orphan object alarm), stored in the C2 centre database (may be manually adjusted)
  - Threshold values for segmentation algorithms, edge detection, change detection and activity detection algorithms, etc.
  - Parameter values (weights, a priori probabilities, etc.) for pattern recognition algorithms.
- Defined Rules for reasoning high level semantics (for scenarios/events to be sought for)
- Parameter values (weights, probabilities, importance factors, etc.) for customizing the "sensitivity" of reasoning rules and the degree of utilization of spatio-temporal co-occurrences of multiple primitive events resulting to a hinted situation insight.

2.4 Identification of useful GE/features proposed by FI-WARE [1]

FI-WARE ref.	GE title	SafeCity Comments	SafeCity Priority
3.2.1	IaaS DataCenter Resource Management	The Video Analytics application would rather not manage such low-level resource management tasks, however this enabler is mandatory lower layer component on top of which the IaaS Service Management resides, which is necessary for the Video Analytics Application	COULD
3.2.2	IaaS Service Management	The Video Analytics Application should be able to define and configure provided virtual resources and their capabilities at a high service level, especially for components requiring real-time processing and are memory-intensive (video processing, reasoning, etc.)	MUST
3.2.3	PaaS Management	It may require a lot of restructuring of the Video Analytics Application so as to use this enabler	WONT
3.2.4	Object Storage	The Video Analytics application may be using this enabler only through other high level invoked enablers – there is no need to directly reference this enabler.	WONT

FI-WARE ref.	GE title	SafeCity Comments	SafeCity Priority
3.2.5	IaaS Cloud Edge Resource Management	Not applicable to the Video Analytics application, from what can be perceived.	WONT
3.2.6	Resource Monitoring	It could be used by the gateway video analytics engine to monitor and pre-process video feeds based on specific metrics so as to single out potentially suspicious content that requires further processing. However, more details are needed in order to judge such applicability of this enabler. It may also be used to measure the efficiency (e.g. near real-time aspect) of the video analytics application, measuring metrics such as response times.	COULD
3.2.7	Resource Metering and Accounting	Same as above	COULD
4.2.1	Publish/Subscribe Broker	It will allow the triggering of further centralized video processing and analysis based on detected (published) suspicious patterns (visual events) in preprocessing at the gateway video feeds.	SHOULD
4.2.2	Complex Event Processing	Very useful for the video analytics application for real-time processing of many video feeds in parallel along with real-time detection/reasoning of threat events over time in each one of the video streams based on defined spatio-temporal rules.	MUST
4.2.3	Big Data Analysis	Fundamental for the video analytics application both for its offline prior events video data processing, pattern recognition and data modeling tasks, as well as for its real-time video stream processing and analysis tasks both at the gateway as well as the centralized C2 system.	MUST
4.2.4	Multimedia analysis	Fundamental for the video analytics application, for both video data and video stream access in various formats as well as their processing and analysis. It further references video processing components (change detection, face detection, etc.) that are included in the video analytics application However more details on the algorithmic selections and processing components (detectors, recognizers, aggregators, etc.) will be much appreciated.	MUST
4.2.5	Unstructured data	Partially useful for the video analytics application in terms of the ontology evolution component	SHOULD

FI-WARE ref.	GE title	SafeCity Comments	SafeCity Priority
	analysis	that is also envisioned in the latter, concerning the SafeCity ontology. The differentiation is that in video analytics ontology evolution is based on detection results of the reasoning process, especially for new types of suspicious behaviours to be incorporated, and in some cases manually assisted annotations.	
4.2.6	Metadata pre-processing	Necessary for accessing metadata and transforming them to the various SafeCity application metadata schemas. It would be useful to add metadata parsing and instantiation/generation capabilities.	MUST
4.2.7	Localization Platform	Not useful for the video analytics application, as it currently stands	WONT
4.2.8	Query Broker	Fundamental with respect to querying the video data and metadata archive used by the Video Analytics application during the detection process as well as for querying the knowledge repository (RDF, will there be provision for OWL-DL?) to reason out semantic information in analyzed video data.	MUST
4.2.9	Semantic Annotation	Not useful for the video analytics application, as it currently stands	COULD
4.2.10	Semantic Application Support	Fundamental with respect to ontology editing and management (to define and update the SafeCity and multimedia Ontologies), querying, reasoning and knowledge repository, It is mentioned that the repository is an RDF-based one and the query language is SPARQL – is there possibility for OWL (-DL) support? A more elaborate description of the capabilities and algorithmic details (e.g. reasoning) will be much appreciated	MUST
4.3.1	Social Network Analysis	N/A for the current version of the video analytics application	WONT
4.3.2	Mobility Analysis	N/A	WONT
4.3.3	Real-time recommendations	N/A for the current version of the video analytics application	WONT
4.3.4	Web behaviour analysis	N/A for the current version of the video analytics	WONT

FI-WARE ref.	GE title	SafeCity Comments	SafeCity Priority
	for profiling	application	
4.3.5	Opinion mining	N/A for the current version of the video analytics application	WONT
5.2.1	USDL Service Descriptions	N/A	WONT
5.2.2	Repository	N/A	WONT
5.2.3	Registry	N/A	WONT
5.2.4	Marketplace	N/A	WONT
5.2.5	Business Models & Elements Provisioning System	N/A	WONT
5.2.6	Revenue Settlement & Sharing System	N/A	WONT
5.2.7	SLA Management	N/A	WONT
5.3.1	Composition editor	N/A	WONT
5.3.2	Mashup execution engine	N/A	WONT
5.3.3	Service orchestration engine	N/A	WONT
5.3.4	Service composition engine	N/A	WONT
5.4.1	Mediation	N/A	WONT
5.4.2	Protocol Mediation	N/A	WONT
5.4.3	Process Mediation	N/A	WONT
5.5.1	Multi-channel/Multi-device Access System	Might be interesting to get video alerts on professional mobile devices (PDA, tablet PC) especially for First Responders on site.	COULD
6.2.1	IoT Communications	Could be used to handle video camera sensors heterogeneity and provide generic access to the respective video feeds (through ARATOS gateway)	SHOULD
6.2.2	IoT Resources Management	Could be used to handle video camera sensors heterogeneity and provide generic access to the respective video feeds (through ARATOS	SHOULD

FI-WARE ref.	GE title	SafeCity Comments	SafeCity Priority
		gateway)	
6.2.3	IoT Data handling	Useful in the Video Analytics application, with respect to the local (gateway) video processing component, content filtering and metadata instantiation	MUST
6.2.4	IoT Process Automation	Very interesting in order to automate the processing and detection process of 6.2.3 (knowledge/rule-driven)	SHOULD
7.2.1	Connected Devices Interfacing (CDI)	N/A for the video analytics application	WONT
7.2.2	Cloud Edge	Useful with respect to the communication interfaces among specific application components and the cloud infrastructure	SHOULD
7.2.3	Network Information and Control (NetIC)	Not directly applicable to the video analytics application	WONT
7.2.4	Service, Capability, Connectivity, and Control (S3C)	N/A	WONT
7.3.1	Security aspects		SHOULD
8.2.1	Security monitoring	It concerns overall communication and system security (incl. video analytics), without however being the primary focus of our application (although mandatory for the entire SafeCity system)	WONT
8.2.2	Identity Management	Useful for the video analytics application in determining which user/device has access to the application	SHOULD
8.2.3	PrimeLife Policy Language (PPL) Engine	Mandatory as video data contain personal data thus privacy issues must be handled.	MUST
8.2.4	Identity Mixer (IdeMix)		WONT
8.2.5	Context-based security and compliance	Could be applied in case of seeking for suspicious behaviours that violate specific people rights	MUST/SHOULD
8.2.6	Optional Security Service Enabler	N/A	WONT

Table 1 Analysis of FI-WARE features/enablers for the Video Analytics Application

2.5 Entries for the FI-PPP backlog

See Cf. Annex : feature backlog entries to check the detail specifications regarding this applications.

2.6 Ask for new features to FI-WARE

It remains to be resolved after more details are provided for the Fi-ware Generic Enablers, what further features and capabilities of the fundamental to be used such enablers will be requested. Some already perceived missing features have been briefly mentioned in Table 2 of Section 3.4.

3. Application 2 "Ad-Hoc Networks" Features and Requirements

3.1 Short Description

Ad hoc networks main objective is to provide effective communication after a catastrophic event happening that disable the typical communication channels. So, ad hoc networks should be quick deployable to provide or restore communication among first responders at the operation field as also communication to the command centre, as soon as possible.

Another objective of the ad hoc networks is to augment capabilities of or replace a communication channel to achieve better service. For example, video can be sent by mobile police patrols to the command centre using an ad hoc network instead of a 3G connection. In this example, it can be increased the video resolution and quality, since a higher bandwidth can be used, as well it can cope the costs of 3G connections.

3.2 Features identification

Ad hoc networks expand network without additional equipment (infrastructure). Ad hoc networks features are the following:

1. Ad hoc nodes addressing
2. Routing between ad hoc nodes
3. Communication independent of the technology (WiFi, WiMAX, TETRA)
4. Support voice, data, image and video transportation
5. Support group communication between ad hoc nodes (access control list, dynamic one to many)
6. Ad hoc nodes location
7. Ad hoc nodes management (remote configuration)
8. Ad hoc nodes coordination (send orders voice, data, image and/or video)
9. Ad hoc nodes resources monitoring (location, battery level, communication stats)
10. Sensors interface (for example, temperature sensor or air quality sensor)
11. Security (authentication, data encryption)

Based on these features, the ad hoc node architecture is represented on Figure 3. It is a layered architecture that includes five layers: application layer, ad hoc node layer, operating system (OS) layer, hardware layer and security layer. The hardware layer includes all physical components for communication, sensors, memories, processors, batteries, and, so on. The OS layer gives an abstraction of the hardware and it is composed by several main functional blocks that should manage memory, processes, communication, resources and files. The ad hoc node layer has the functions regarding ad hoc networks, including routing, self-configuration, remote configuration, sensors manager, quality of

service functions and so on. The application layer allows the execution of applications that take advantage of lower layers. For example, sensors data can be monitored and transmitted through the ad hoc network. Other application example, ad hoc nodes can communicate among them using VoIP. Transversal to all the layers explained before, the security layer provides security features to any layer such as authentication, authorization, encryption, integrity, and so on.

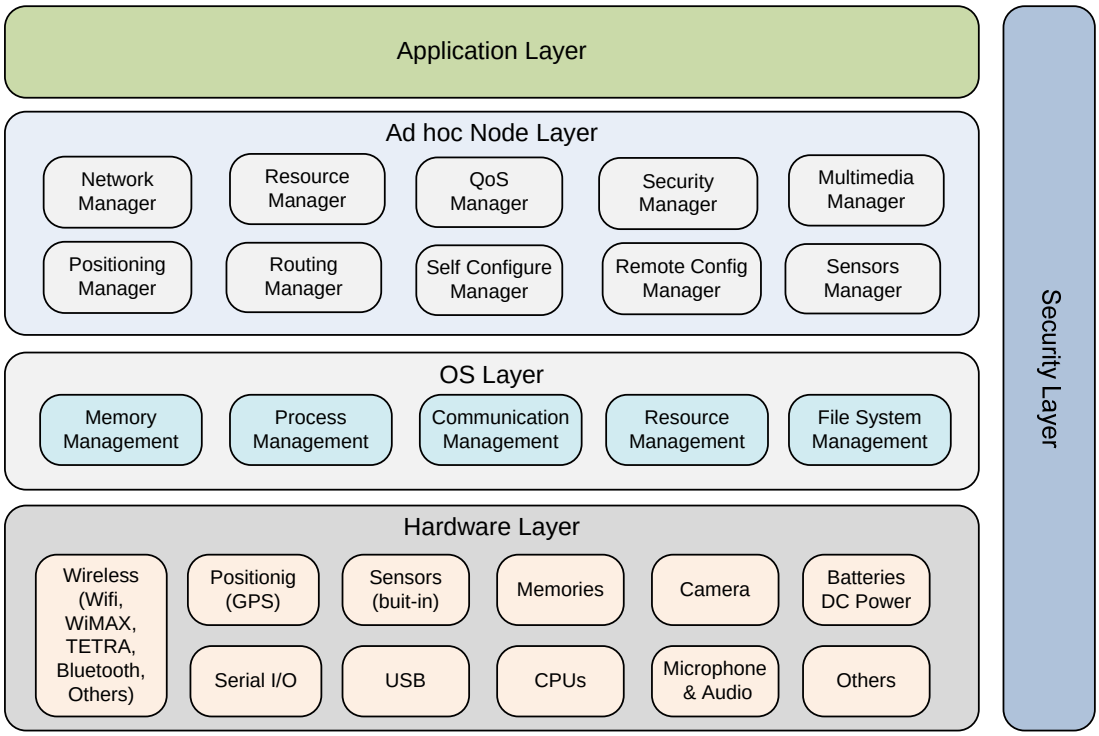


Figure 3 Ad hoc node architecture

The Figure 4 presents an example of an ad hoc network deployed on a city after a disaster. Each sensor node can have several sensors connected and it transmits the sensors data through the ad hoc network up to the SafeCity using the gateway nodes. The ad hoc network is built dynamically and automatically, the nodes are able to self-configure themselves. Furthermore, there could be some specific applications for the authorities to coordinate and exchange data among them regarding public safety and disaster recover. Also, the ad hoc nodes can interface with some specific public safety applications of citizens for alerting them, for example, the applications can be running on citizens' smartphones with multiple communication interfaces. The SafeCity system, deployed on a public or private cloud, can be interfaced using gateway nodes and, this way, it is possible to the SafeCity system obtains information from sensors and from local command and control centres though polling services. As well, citizens can interact directly with the SafeCity system to receive warnings and alerts directly from it, if the SafeCity system is available.

Legend:
(1) – Ad-hoc network for sensor connection, capacity augmentation or replacement after disasters
(2) – Applications for Authorities
(3) – Applications for Citizens
(4) – C2 and sensor polling services
(5) – Warning dissemination services

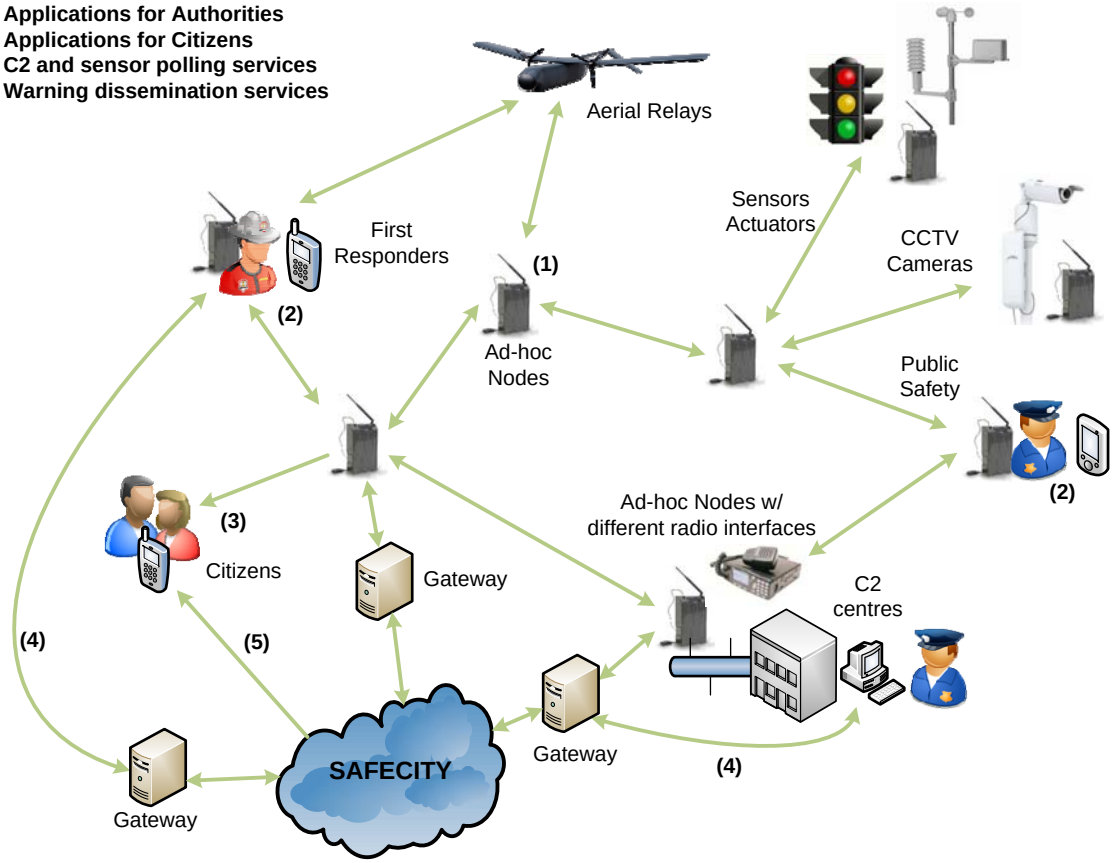


Figure 4 – Ad hoc network deployment example

3.3 Requirements

Requirements	Generic Expression	Expression of requirements within the scope of the 1st WP4 trials
Routing protocols	OLSR	OLSR
Nodes Addressing	IPv4 based	IPv4 based
Technologies of Communication	WiFi, WiMAX, TETRA	WiFi
Voice requirements	Bandwidth: <100kbps (CODEC dependent) Latency: low Jitter: low	Bandwidth: <100kbps (CODEC dependent) Latency: low Jitter: low
Sensors data requirements	Bandwidth: <1kbps (sensor dependent) Latency: not relevant Jitter: not relevant	Bandwidth: <1kbps (sensor dependent) Latency: not relevant Jitter: not relevant
Image requirements	Bandwidth: <100kbps (image resolution dependent) Latency: medium Jitter: not relevant	Bandwidth: <100kbps (image resolution dependent) Latency: medium Jitter: not relevant

Video requirements	Bandwidth: ~1Mbps (video resolution and CODEC dependent) Latency: low Jitter: low	Bandwidth: ~1Mbps (video resolution and CODEC dependent) Latency: low Jitter: low
Location requirements	GPS (latitude, longitude, altitude, speed) GPS accuracy: <10m	GPS (latitude, longitude, altitude, speed) GPS accuracy: <10m
Group communication	Inter-agency communication with dynamic one-to-many communication	Inter-agency communication with dynamic one-to-many communication
Security requirements	Authentication to be part of the ad hoc network Data encryption	Optional

Table 2 Requirements for the Ad Hoc Network Application

3.4 Identification of useful GE/features proposed by FI-WARE [1]

FI-WARE ref.	GE title	SafeCity Comments	SafeCity Priority
3.2.1	IaaS DataCenter Resource Management	Not applicable to ad-hoc networks.	WONT
3.2.2	IaaS Service Management	Not applicable to ad-hoc networks.	WONT
3.2.3	PaaS Management	Not applicable to ad-hoc networks.	WONT
3.2.4	Object Storage	Not applicable to ad-hoc networks.	WONT
3.2.5	IaaS Cloud Edge	Not applicable to ad-hoc networks.	WONT
3.2.6	Resource Monitoring	Not applicable to ad-hoc networks.	WONT
3.2.7	Resource Metering and Accounting	Not applicable to ad-hoc networks.	WONT
4.2.3	Big Data Analysis	Handle data, voice, video and images from ad-hoc network devices.	COULD
4.2.2	Complex Event Processing	Real-time communication with command and control center, where the decisions are made.	COULD
4.2.4	Multimedia analysis to gather multimedia meta-data	Not applicable to ad-hoc networks.	WONT
4.2.6	MetaData preprocessing	Not applicable to ad-hoc networks.	WONT
4.2.5	Unstructured data analysis	Not applicable to ad-hoc networks.	WONT
4.2.6	Localization Platform	The location of ad-hoc nodes can contribute to decision making.	MUST

FI-WARE ref.	GE title	SafeCity Comments	SafeCity Priority
4.2.7	Query-access	Query data of ad hoc nodes from sensors including, also, video and images.	COULD
4.2.8	Broker	Configure how to collect data from ad hoc sensor nodes (publish/subscribe).	COULD
4.2.9	Semantic Annotation enabler	Not applicable to ad-hoc networks.	WONT
4.2.10	Semantic Application Support enabler	Not applicable to ad-hoc networks.	WONT
4.3.1	Social Network Analysis	Not applicable to ad-hoc networks.	WONT
4.3.2	Mobility Analysis	Ad hoc network can provide data to the decision support system for the mobility analysis of the ad hoc nodes.	COULD
4.3.3	Real-time recommendations	Ad hoc nodes could receive real time recommendations regarding safety issues from the command and control centre.	COULD
4.3.4	Web behaviour analysis for profiling	Not applicable to ad-hoc networks.	WONT
4.3.5	Opinion mining	Not applicable to ad-hoc networks.	WONT
5.2.1	USDL Service Descriptions	Not applicable to ad-hoc networks.	WONT
5.2.2	Model Repository	Not applicable to ad-hoc networks.	WONT
5.2.3	Service Registry	Not applicable to ad-hoc networks.	WONT
5.2.4	Marketplace	Not applicable to ad-hoc networks.	WONT
5.2.5	Business Models & Elements Provisioning System	Not applicable to ad-hoc networks.	WONT
5.2.6	Revenue Settlement & Sharing System	Not applicable to ad-hoc networks.	WONT
5.2.7	SLA Management	Not applicable to ad-hoc networks.	WONT
5.3.1	Composition editor	Not applicable to ad-hoc networks.	WONT
5.3.2	Composition execution engines	Not applicable to ad-hoc networks.	WONT

FI-WARE ref.	GE title	SafeCity Comments	SafeCity Priority
5.5.1	Multi-channel/Multi-device Access System	Not applicable to ad-hoc networks.	WONT
6.2.1	IoT Communications	Ad hoc nodes networks must be aware of connectivity management (disconnect issues, for example), incoming/outgoing traffic from each device, traffic flow management, access control and quality of service.	MUST
6.2.2	IoT Resources Management	Ad hoc nodes must include management functions for resource identification, nodes discovery (resource or service based) and interact with sensors/actuators connected to each node.	MUST
6.2.3	IoT Data handling	Provide the data exchange among ad hoc nodes and command centres. The data management involves nodes local storage, data access management, real-time data accesses, mechanisms to access data (publish, subscribe and notify) and data integration issues.	MUST
6.2.4	IoT Process Automation	It could be useful to specify some low level business processes to execute among ad hoc nodes.	COULD
7.2.1	Connected Devices Interfacing (CDI)	CDI GE detects and exploits capabilities, resources, contents and contextual information of ad hoc nodes status using a specific API located on each device.	SHOULD/MUST
7.2.2	Cloud Edge	Ad hoc nodes connection to the Gateway.	MUST
7.2.3	Network Information and Control (NetIC)	It provides ad hoc network information status and ad hoc network control and management capabilities. Interesting functions regarding ad hoc networks: topology, interface control, path statistics and control, traffic statistics and control.	MUST
7.2.4	Service, Capability, Connectivity, and Control (S3C)	Ad hoc networks are also packet core network. S3C GE will offer API interesting for ad hoc networks: network event management, resource management, network identity management, connectivity management, and security functions.	COULD
7.3.1	Security aspects	Mandatory	MUST

FI-WARE ref.	GE title	SafeCity Comments	SafeCity Priority
8.2.1	Security monitoring	Ad hoc nodes can be part of the security system, providing information regarding security. It should be a lightweight process.	COULD
8.2.2	Identity Management	Ad hoc nodes should provide authentication mechanisms to prevent that stolen or lost devices interfere on the system.	SHOULD/MUST
8.2.3	PrimeLife Policy Language (PPL) Engine	Not applicable to ad-hoc networks.	WONT
8.2.4	Identity Mixer (IdeMix)	Not applicable to ad-hoc networks.	WONT
8.2.5	Context-based security and compliance	Not applicable to ad-hoc networks.	WONT
8.2.6	Optional Security Service Enabler	Some optional security services could be used (data encryption).	COULD

Table 3 Analysis of FI-WARE features/enablers for the Ad Hoc Network Application

3.5 Entries for the FI-PPP backlog

See Cf. Annex : feature backlog entries to check the detail specifications regarding this applications.

3.6 Ask for new features to FI-WARE

Majority of required features for ad hoc network application are addressed by FI-WARE. These features will be provided by FI-WARE using specific API that will be installed on devices (ad hoc nodes).

The following features are important to ad hoc network application:

- Ad hoc nodes addressing may be implemented through GE NetIC (7.2.3) or GE S3C (7.2.4), but it is not clear how this feature are targeted.
- Ad hoc nodes routing protocol considering device location and energy level is a feature that should be provided.

4. Application 3 "Intelligent Sensors and Information Pre-Processing" Features and Requirements

4.1 Short description

The application is going to distribute some of the operational and processing logic developed in C2 premises to the sensor network on the field. The idea is to enable intelligent synchronization of the sensor outputs, based on early definitions of detected alerts, so as to optimize QoS and data fusion on a higher level.

The application does not aim to substitute the centralized data fusion and video analytics processes to be realized as key tools for the detection and evaluation of abnormalities. Instead it shall use some these rules to embedded intelligence, so as to force network traffic criteria with respect to the C2 priorities.

So, for example, if two out of the ten cameras in an area detect an abnormality, the outputs from these two sensors should be transmitted with increased priority and perhaps even combined, so as to tell a first estimation story. Later, in the C2 centre, a holistic situational awareness and detailed analysis of the alerts detected shall be realized, based upon all the inputs received, advanced processing algorithms and decision-making modules.

Achievements

The application design aims in achieving the following points:

- ✓ Early detection of a potential alert, at the instance this is being monitored;
- ✓ Early combination of sensor outputs telling a potential story, alerts to be transmitted as logic information packages, based upon context awareness;
- ✓ Controlling network traffic priorities and QoS based on sensor output, so as to manage a challenging city-wide network of infinite interconnected nodes;
- ✓ Distributing processing logic to the edges of the network and down to the sensor-level, enabling the delivery of outputs enriched with metadata
- ✓ Shifting some of the C2 work overload to the network routers, relieving the management of *raw* , heavy information load

4.2 Features identification

The following diagram presents the architecture design of the application:

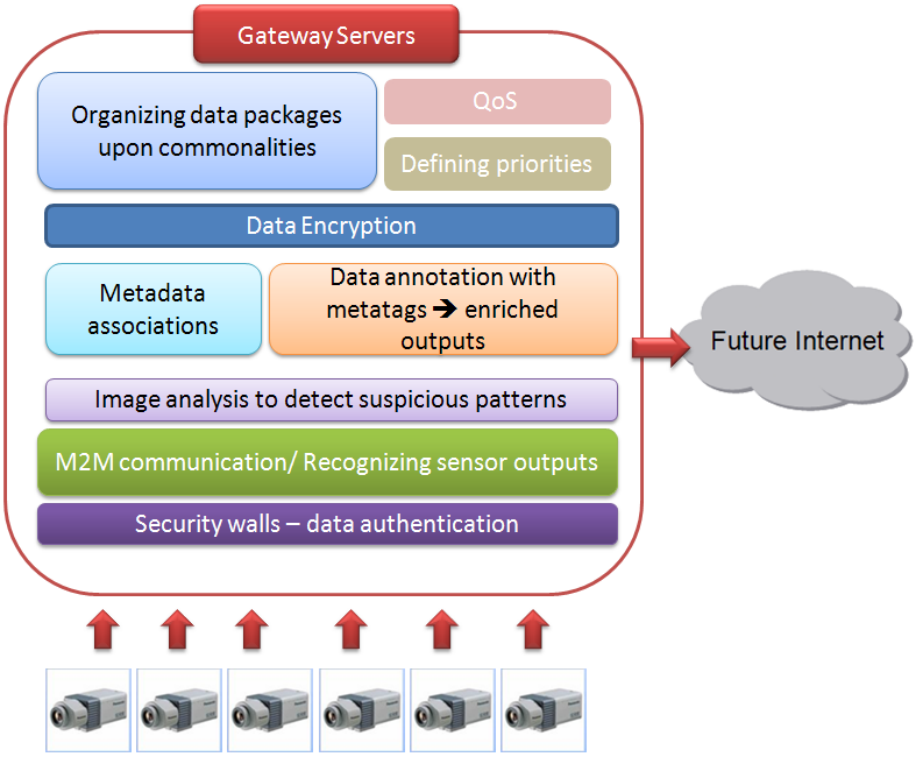


Figure 5 Features of the Gateway application

Functionalities:

The application is also referred to as the "Gateway Application" because it is going to be implemented in Gateway servers. Seeing that the application is going to control the synchronization and QoS of the sensor outputs, this seems to be a valid design.

The application will try and accept all sensor outputs received per close time intervals and process them individually, as well as with regard to the others. Therefore, the first necessary module for the application is the introduction of M2M communication, so as to enable the effective integration of all data types, sources, sensor families, etc. Of course, data integration will be secured by authentication mechanisms, ensuring that no malicious injection and unauthorized sources are being involved.

Then, all data are being subject to image analysis techniques to detect suspicious patterns, miming basic considerations of the video analytics application running on the C2 centre. Low level image analysis is going to be realized. The processing capabilities shall not be as powerful as the ones deployed in the C2 stations, but they will be able to detect suspicious patterns based on a set of pre-defined attributes to be looked for. If a sensor image is detected as such, it will be enriched with metatags indicating so. The metatags annotation will be in reference with the SafeCity ontology, so as to ensure compliance with the data processing and fusion modules in C2 centres. SO, based on the findings generated, the original outputs are being enriched with a new series of metadata, indicating their detected alerts.

A series of intelligent estimations shall be realized in order to determine which data should be prioritized (based on indication of alerts) and which data should be combined (based on common patterns detected, synchronization, location, etc).

Based on this process, the data are being prioritized and combined, based on QoS rules and mechanisms following C2 considerations and criteria. Of course, prior to transmitting information across the main network, encryption mechanisms take place to protect their content.

4.3 Identified requirements

Requirements	Generic Expression	Expression of requirements within the scope of the 1st WP4 trials
Bandwidth support	Similar to the original requirements for video inputs	
Metadata	Timestamp and location in 3D, information upon the sensor device (type, manufacturer,)	Timestamp and location in 3D
Recognition of new nodes, mobility and network re-configurability	Ability to detect new sensors/actuators and align them to the integration platform. This means that the application needs to integrate with new Ad-Hoc sensors automatically	Tracing on new ad-hoc and mobile sensors
SafeCity Ontology Definition	Definition of common set of metadata in regard to definition of suspicious patterns, etc.	Definition of common set of metadata in regard to definition of suspicious patterns, etc.
Search Engine	To allow searches upon a specific value/ metacontent	Optional
Security: De-encryption Mechanisms	Data being handled by the application are going to temporarily platform, be processed and then sent to the C2 station with actual information alerts. Extra caution is needed during the entire path that data follows	Security levels to be introduced across the intermediate states of the sensors outputs (original output→ pre-processed output→C2 center)
Security: Encryption Mechanisms		
Security: Authentication access	Authentication access shall allow only a restricted group of individuals and sensors to interact	Necessary for demonstration with Ad-hoc sensors
IoT	Ability to see and detect nodes	Metatags definitions are going to be used to allow an xml-based communication
Scalable computing power and storage	In order to cope effectively with scaling amount of data received and processing needs, the supporting hardware needs to be alternate accordingly, so as to optimize cost and latency requirements	Cloud edge, secured with encryption mechanisms to be used Storage requirements, typically similar to data fusion requirements
Privacy requirements	Same as video analytics application	
Processing Latency	Mechanisms to minimize processing latency, so that the extra processing stage shall not burden the network significantly	Optional

Network Latency	Network latency needs to be kept to minimum levels, so as to guarantee that the pre-processing metadata rich the C2 center prior to losing their effect	Slightly lower than the requirements set by C2 applications, so as to care for processing latency within the application

Table 4 Requirements for the intelligent sensors and pre-processing application

4.4 Identification of useful GE/features proposed by FI-WARE [1]

FI-WARE ref.	GE title	SafeCity Comments	SafeCity Priority
3.2.1	IaaS DataCenter Resource Management		MUST
3.2.2	IaaS Service Management		COULD
3.2.3	PaaS Management		COULD
3.2.4	Object Storage		SHOULD
3.2.5	Cloud Edge		SHOULD
3.2.6	Monitoring		SHOULD
3.2.7	Resource Metering and Accounting		COULD
4.2.1	Big Data Processing		MUST
4.2.2	Complex Event Processing		MUST
4.2.3	Multimedia analysis to gather multimedia meta-data		MUST
4.2.4	Pre-processing of meta-data during/after gathering		SHOULD
4.2.5	Preprocessing of unstructured data during/after gathering		SHOULD
4.2.6	Localization Platform		MUST
4.2.7	Query-access		SHOULD
4.2.8	Publish/Subscribe Broker		SHOULD

FI-WARE ref.	GE title	SafeCity Comments	SafeCity Priority
4.2.9	Semantic Annotation enabler	-	MUST
4.2.10	Semantic Application Support enabler	-	MUST
4.3.1	Social Network Analysis	-	COULD
4.3.2	Mobility Analysis	-	COULD
4.3.3	Real-time recommendations	-	WONT
4.3.4	Behavioural and Web profiling	-	WONT
4.3.5	Opinion mining	-	WONT
5.2.2	USDL Service Descriptions	-	SHOULD
5.2.3	Model Repository	-	COULD
5.2.4	Service Registry	-	WONT
5.2.5	Marketplace	-	WONT
5.2.6	Business Models & Elements Provisioning System	-	WONT
5.2.7	Revenue Settlement & Sharing System	-	WONT
5.2.8	SLA Management	-	MUST/SHOULD
5.3.3	Composition editor	-	COULD
5.3.4	Application mashup editor	-	COULD
5.3.5	Service composition editor	-	COULD
5.3.6	Execution engine	-	COULD
5.3.7	Mashup execution engine	-	COULD
5.3.8	Service composition	-	COULD

FI-WARE ref.	GE title	SafeCity Comments	SafeCity Priority
	engine		
5.3.9	Service orchestration engine	-	COULD
5.3.10	Aggregator repository	-	COULD
5.4.1	Data Mediation	-	SHOULD
5.4.2	Protocol Mediation	-	SHOULD
5.4.3	Process Mediation	-	SHOULD
5.5.1	Multi-channel/Multi-device Access System	-	WONT
6.2.1	IoT Communications	-	MUST
6.2.2	IoT Resources Management	-	COULD
6.2.3	IoT Data handling	-	SHOULD
6.2.4	IoT Process Automation	-	SHOULD
7.2.1	Connected Devices Interfacing (CDI)	-	SHOULD
7.2.2	Cloud Edge	-	SHOULD
7.2.3	Network Information and Control (NetIC)	-	SHOULD
7.2.4	Service, Capability, Connectivity, and Control (S3C)	-	SHOULD
7.3.1	Identity and privacy management	-	SHOULD
8.2.1	Security monitoring	-	MUST
8.2.2	Identity Management	-	COULD
8.2.3	PrimeLife Policy Language (PPL) Engine	-	COULD
8.2.4	Identity Mixer (IdeMix)	-	COULD

FI-WARE ref.	GE title	SafeCity Comments	SafeCity Priority
8.2.5	Context-based security and compliance	-	SHOULD
8.2.6	Optional Security Service Enabler	-	SHOULD

Table 5 Analysis of FI-WARE features/enablers for the intelligent sensors and pre-processing application

4.5 Entries for the FI-PPP backlog

See Cf. Annex : feature backlog entries to check the detail specifications regarding this applications.

5. Application 4 "Real-time Positioning based on video analysis and artificial intelligence for decision support": Features and Requirements

5.1 Short description

Based on a **3D model of the town**, The SafeCity project will offer a 2D/3D view of the town, representing people in the town. Two kinds of information will be included:

- 3D position of people in real time extracted by video analysis.
- 3D position and behavior of people, obtained by artificial intelligence algorithms, when real information is not available.

Video Analysis

Based on an existing camera network or on deployed camera network, with space covered by more than one camera, video analysis will extract people tracking information. Thales tracking solution stresses on ease of network deployment and cameras calibration and has the advantage of giving a 3D position (vs. 2D for most solutions).

Artificial intelligence

Based on real life information coming from video analysis and on crisis situation crowd modeling knowledge, a functionality of anticipation of people actions is developed. More precisely, two scales of behavior simulation will be proposed: The ability to anticipate the path and the next actions of a pointed out person and the ability to anticipate a crowd movement after an incident.

Achievements

Thales supervision tool will offer functionalities such as:

- Ability to track a pointed out person
- Ability to anticipate a pointed out person path
- Ability to propose possible paths followed by a pointed out person (for forensic purposes)

The primary use of this tool will be to support decision making after an event such as a crime, an accident or a disaster.

5.2 Features identification

Features represented in dark blue are features that will be demonstrated in Application 4. Other features represented in grey are additional needed features to run this kind of application in an operational environment, in order to enable for example forensic in addition or real-time video protection.

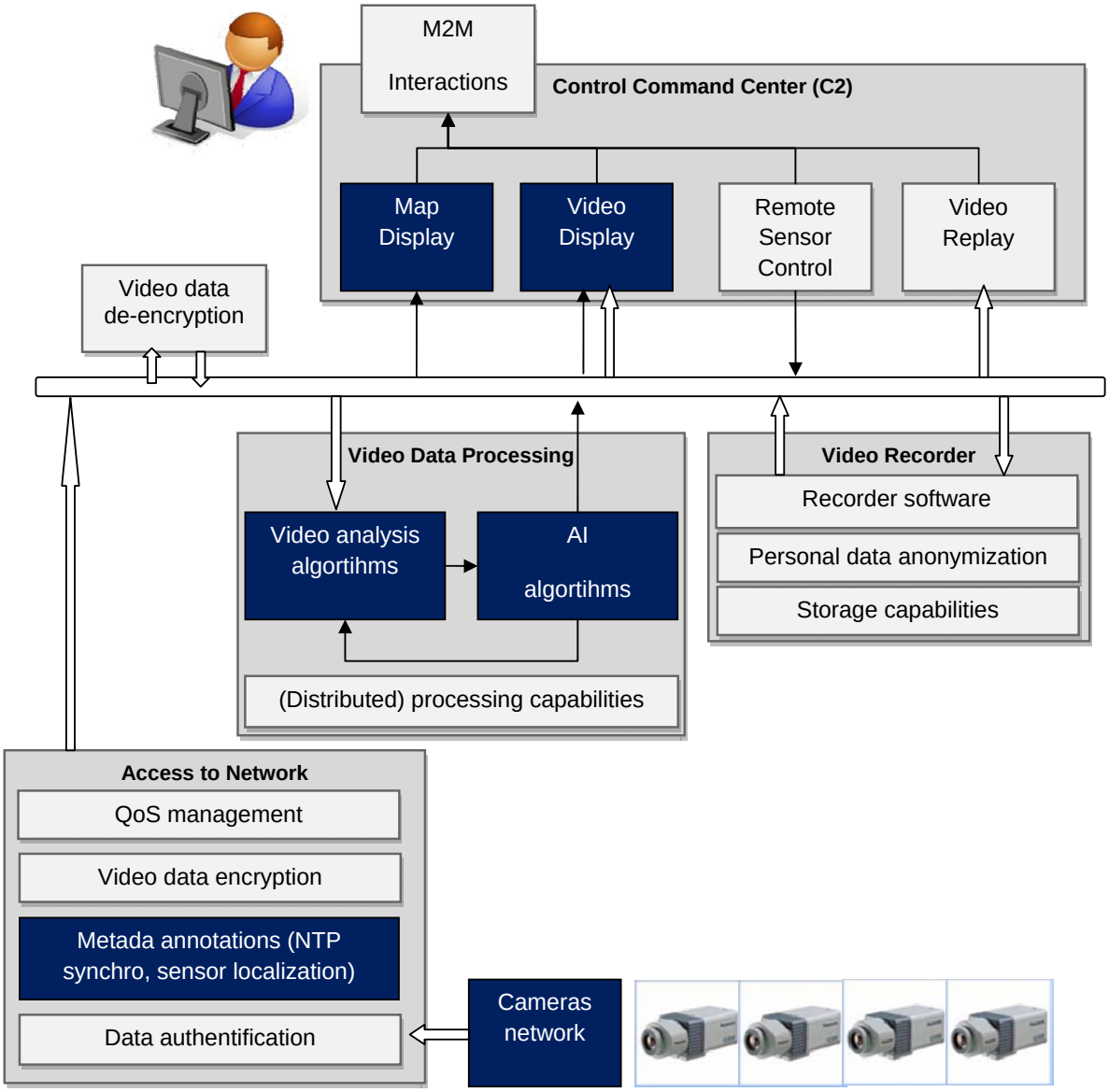


Figure 6 Real Time positioning application features

The main technical features are described below:

- **Map Display**: Ability to display a map of the city with 2D (and 3D) views. This module offers zoom capabilities and possibility to change from 2D to 3D view in order to focus on a specific zone (once the zoom level is big enough)
- **Video Display**: Ability to display on one video wall all the CCTV streams. This module also offers the capability to the operator to select only relevant videos to display.
- **AI algorithms**: Ability to compute probability of path for people and/or cars
- **Video Analysis Algorithms** : Ability to track people and/or cars through a camera network (Note: In fact, people/cars tracking capability through a camera network is given via both video analysis and AI capabilities)
- **Map Display**: Ability to display a map of the city with 2D (and 3D) views. This module offers zoom capabilities and possibility to change from 2D to 3D view in order to focus on a specific zone (once the zoom level is big enough). The results of Video analysis and AI algorithms can also be displayed on the map.

- **Video Display**: Ability to display on one video wall all the CCTV streams. This module also offers the capability to the operator to select only relevant videos to display. The results of Video analysis and AI algorithms can also be displayed on the video wall.
- **Stream Tag**: Video stream time synchronization capabilities
- **Sensors**: sensors are CCTV cameras, with known position in a 3D environment (x, y, z, pan, tilt, roll)
- **Remote Sensor Control**: Ability to remotely control CCTV sensors (asks for stream transmission and control Pan/Tilt/Zoom).
- **Video Replay**: capacity to replay part of the video giving one sensor identifier, one start date, and one duration
- **Video Recorder**: capacity to store video data and associated metadata

5.3 Requirements

In this section, technical requirements have been identified in two parts, first, a table presents requirements dealing with network, and a second part presents more specific requirements regarding the set up of the application itself.

The first table below presents requirements dealing with network, considering in the first column the ability to run this application in the overall city environment, and considering in parallel in the second column the subset of requirements in order to run experimentation and first trials in WP4.

Requirements	Generic Expression	Expression of requirements within the scope of the 1st WP4 trials
Video Quality Requirement	In order to perform video analysis: • Image quality : 4CIF (or VGA) • Video compression: H264 or MJPEG (preference to MJPEG) • 8-12 images/sec (=>Compression rate 8 to 48)	In order to perform video analysis: • Image quality : 4CIF (or VGA) • Video compression: H264 or MJPEG (preference to MJPEG) • 8-12 images/sec (=>Compression rate 8 to 48)
Bandwidth requirements	Assumptions: 100 to 8 000 cameras • 2Mbits/sec to 8Mbits/sec per stream	Assumptions : 30 cameras for the demonstration • 2Mbits/sec to 8Mbits/sec per stream
Stream synchronization	In order to perform tracking algorithms through a camera network, video streams coming from different cameras must be synchronized.	Video streams coming from various sensors must be synchronized with a common time reference through the network (timestamp in the encoding diagram, NTP server)
Privacy requirements	Personal data (faces, number plates..) contained in the video must be protected from illegal access	No need for the demo.
MetaData	In addition of timestamp, MetaData must contain sensor location information in 3 dimensions	3D position of sensors can be known a priori for the demonstration
Automatic discovery of sensors/actuators	A service discovery mechanism	Optional

connected		
Security Requirements	New sensor and user must be authenticated before having access to applications, devices.Access level to applications, device, ad-hoc network must be dynamically configurable	Optional
Quantity of data	1 week of system nominal behavior data record (for learning and calibration)	1 day of system nominal behavior data record

Table 6 Requirements for the Real Time Positioning Application

As other specific requirements in order to set up real-time positioning application, we can list:

- Need of a 3D model in the Collada format (or .OBJ is possible) of the part of the town in which the application will be set up
- 1 Tera of video recording and storage space is needed for 20 cameras
- a PC server for 2 cameras is needed and one PC is needed for the AI algorithms
- Field of view of cameras has to be static and the position and orientation has to be known with enough precision in the 3D model.

5.4 Identification of useful GE/features proposed by FI-WARE [1]

FI-WARE ref.	GE title	SafeCity Comments	SafeCity Priority
3.2.1	IaaS DataCenter Resource Management	VM hosting capabilities are mandatory. Secure access to VM is mandatory as well.	MUST
3.2.2	IaaS Service Management	Definition and Configuration of virtual resources capabilities are mandatory. CPU / shared memory capabilities are very important for the quality of the AI services	MUST
3.2.3	PaaS Management	Not compliant (our application is not compliant, we manage internally our application lifecycle).	WONT
3.2.4	Object Storage	This 3.2.4 description is very technical and not very clear to us by now.	WONT
3.2.5	IaaS Cloud Edge	Do not see the added value of this 3.2.5 GE compared to existing ADSL box/NAS.	WONT
3.2.6	Resource Monitoring	To study when detailed.	
3.2.7	Resource Metering and Accounting	To study when detailed.	
4.2.3	Big Data Analysis	Very useful for video data streaming, processing and storage, According to the developed AI system technical design, it may request the	MUST/SHOULD COULD/SHOULD

FI-WARE ref.	GE title	SafeCity Comments	SafeCity Priority
		support of such a GE. To study when detailed.	
4.2.2	Complex Event Processing	Can be useful in a security system, not especially for this application 4. According to the developed AI system technical design, it may be very useful to exploit such a GE.	COULD, SHOULD/MUST
4.2.4	Multimedia analysis to gather multimedia meta-data	It would be more interesting to provide an API for embedded 3rd party "media stream analysis", (Indeed, this function is business specific). "Media interface" and "metadata interface" are interesting.	SHOULD
4.2.6	MetaData preprocessing	OK.	SHOULD
4.2.5	Unstructured data analysis	Not useful for our application.	WONT
4.2.6	Localization Platform	Not useful for this version of our application.	WONT(/COULD)
4.2.7	Query-access	Would be interesting if add video query. Could be interesting with semantic queries are possible about the gathered data, also if there is some topological (geographical or positioning) queries available	COULD
4.2.1	Broker	Does it include new sensors connected to the network discovery? Will it be environment specific? Useful for behavior analysis and AI inputs and outputs. The events should be correlated to object (ID) and timestamped.	SHOULD
4.2.9	Semantic Annotation enabler	Not useful for this version of our application. Could have been useful if it was possible to associate semantic annotation to geometric representation of the environment (not only text-based data), in order to designate landmarks, for instance (road, sidewalk, pedestrian crossings, etc.)	WONT(/COULD)
4.2.10	Semantic Application Support enabler	Not useful for this version of our application. (if text-based only)	WONT(/COULD)
4.3.1	Social Network Analysis	Not useful for our application.	WONT
4.3.2	Mobility Analysis	Not useful for this version of our application. Users points of interest and frequents itineraries between these points of interest could be very	WONT(/COULD) COULD

FI-WARE ref.	GE title	SafeCity Comments	SafeCity Priority
		useful to predict behaviors of observed people	
4.3.3	Real-time recommendations	Not useful for our application.	WONT
4.3.4	Web behaviour analysis for profiling	Not useful for our application.	WONT
4.3.5	Opinion mining	Not useful for our application.	WONT
5.2.1	USDL Service Descriptions	Not useful for this version of our application.	WONT(/COULD)
5.2.2	Model Repository	Not useful for our application.	WONT
5.2.3	Service Registry	Not useful for this version of our application. Useful if several Police force department need to access to the video-protection service.	WONT(/COULD)
5.2.4	Marketplace	Not useful for our application.	WONT
5.2.5	Business Models & Elements Provisioning System	Not useful for our application.	WONT
5.2.6	Revenue Settlement & Sharing System	Not useful for our application.	WONT
5.2.7	SLA Management	Very useful to guarantee QoS like bandwidth, or CEP real-time response	MUST/SHOULD
5.3.1	Composition editor	Not useful for our application.	WONT
5.3.2	Composition execution engines	Not useful for our application.	WONT
5.5.1	Multi-channel/Multi-device Access System	Might be interesting to get video on professional mobile devices (PDA)	COULD
6.2.1	IoT Communications	Interesting to handle sensor heterogeneity	SHOULD
6.2.2	IoT Resources Management	Interesting to handle sensor heterogeneity	SHOULD
6.2.3	IoT Data handling	Interesting to handle small sensor heterogeneity	COULD
6.2.4	IoT Process Automation	Interesting to connect sensor with business processes Need precision: what is the difference with 5.4.1	COULD/SHOULD

FI-WARE ref.	GE title	SafeCity Comments	SafeCity Priority
7.2.1	Connected Devices Interfacing (CDI)	Might be interesting to get video on professional mobile devices (PDA)	COULD
7.2.2	Cloud Edge	Cf. 3.2.5	
7.2.3	Network Information and Control (NetIC)	Mandatory. Bandwidth prior access management for First responders and Police Force. (not useful for AI, even if I wonder why these functionalities aren't embedded in the IaaS?)	MUST
7.2.4	Service, Capability, Connectivity, and Control (S3C)	Not useful for our application. But interesting for Safety use case.	WONT
7.3.1	Security aspects	Mandatory	MUST
8.2.1	Security monitoring	Mandatory	MUST
8.2.2	Identity Management	Mandatory. Manage device and application access right. X	MUST
8.2.3	PrimeLife Policy Language (PPL) Engine	Mandatory (video contain personal data, privacy issues to handle). This enabler will allow configuring video data access right. Also needed as we will gather information about path and habits of people, even if we can do that anonymously, we should be able to prove it legally	MUST/COULD
8.2.4	Identity Mixer (IdeMix)	Could be useful.	COULD
8.2.5	Context-based security and compliance	Very interesting	MUST/SHOULD
8.2.6	Optional Security Service Enabler		WONT

Table 7 Analysis of FI-WARE features/enablers for Real-time Positioning Application

5.5 Entries for the FI-PPP backlog

See Cf. Annex : feature backlog entries to check the detail specifications regarding this applications. Prior entries for the real-time positioning application deal with multimedia analysis GE (regarding the video analysis part of the application) and with the CEP GE (regarding the AI part of the application).

5.6 Ask for new features to FI-WARE

In this sub-chapter, some interesting functions that would be very interesting for the real-time positioning application are listed. These functions are not provided or not clearly provided by the Core

Platform by now, so they are listed below in order to keep them in mind and propose them as generic enablers:

- Video encryption: to enable personal data (faces, number plates, etc.) transmission with Law compliancy.
- Video anonymization: to enable personal data (faces, number plates, etc.) storage with Law compliancy.
- Dynamic access right and QoS configuration: Access level to applications, device, ad-hoc network must be dynamically configurable, depending of the situation (crisis, incident, normal) and of the people (people , Police force level 1, Police force level 2, First responders level 1, etc.)

6. Application 5 “Data Fusion” Features and Requirements

6.1 Short description

Data Fusion will be a technology placed at the core of C2 Centers, serving as key decision support tool. Based on data gathered by SafeCity applications, such as Video Analytics, 3D mapping or intelligent sensors, by third party data providers or external databases, this application shall provide a set of functionalities that will help in understanding and correlating heterogeneous information generated by any mean and any place into SafeCity in order to extract its meaning and make it easily available for Decision Support System, Human operators or any other application through an API.

Achievements

To realize this module, several previous steps need to be followed:

- SafeCity Ontology definition so that any event, document or instance can be classified and indexed according to this Ontology. This ontology will be built based on final users requirements, applications requirements and previous works and standards on this area.
- Ability to store terns (semantic metadata) and link to the data source (reference metadata) in a database.
- Ability to infer new knowledge using Reasoner Engine.
- Ability to perform manual annotation, generating enrich knowledge which can be further exploited not only to provide the requested content, but also to enrich results with additional , yet meaningful content.
- Ability to perform queries showing matches elements and relationships between them using Search Engine.

6.2 Features identification

In order to obtain the above achievement we should use technologic enablers. These enablers and their relations with specific Data Fusion module are shown below.

- Ability to define and modify SafeCity Ontology so that any event, document or instance can be classified and indexed according to this Ontology. This functionality should be provided by Semantic Application Support enabler, accordingly to FI-PPP, concretely with Semantic Engineering module.

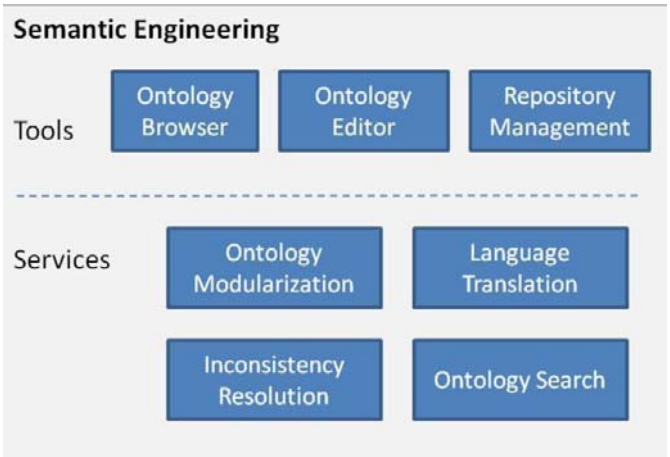


Figure 7 Schematic view Semantic Engineering layer

- Ability to store terns into repository. This functionality should be provided by Semantic Application Support enabler, accordingly to FI-PPP, concretely should be provided by Semantic Infrastructure module (Repository). Furthermore due the vast amount of data to store and the need to use effective storage systems with advanced functionalities or some other enablers could be considered, like cloud database enabler.

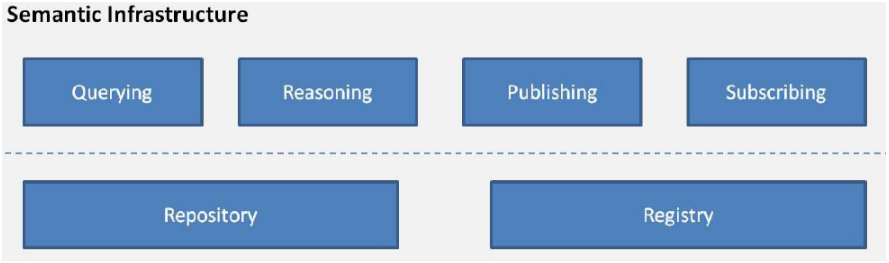


Figure 8 Schematic view Semantic Infrastructure layer

- Ability to infer new knowledge using Reasoner Engine. From previous stored knowledge this module generates/infers new knowledge. This functionality should be provided by Semantic Application Support enabler, accordingly to FI-PPP, concretely should be provided by Semantic Infrastructure module (Reasoning). Moreover taking account the large amount of data, inferred new knowledge can be computationally costly, therefore IaaS Service Management enabler for cloud computing could be used in order to instantiate additional Reasoning resources.
- Ability to performs manual annotation, generating enrich knowledge which can be further exploited not only to provide the requested content, but also to enrich results with additional , yet meaningful content.
- Ability to perform queries showing matches elements and relationships between them using Search Engine. This functionality should be provided by Semantic Application Support enabler, accordingly to FI-PPP, concretely should be provided by Semantic Infrastructure module (Querying).

Finally, in order to provide a global vision's module and their relationship with other enablers also the relation between them a general high architectural vision of DataFusion module is showed in following figure

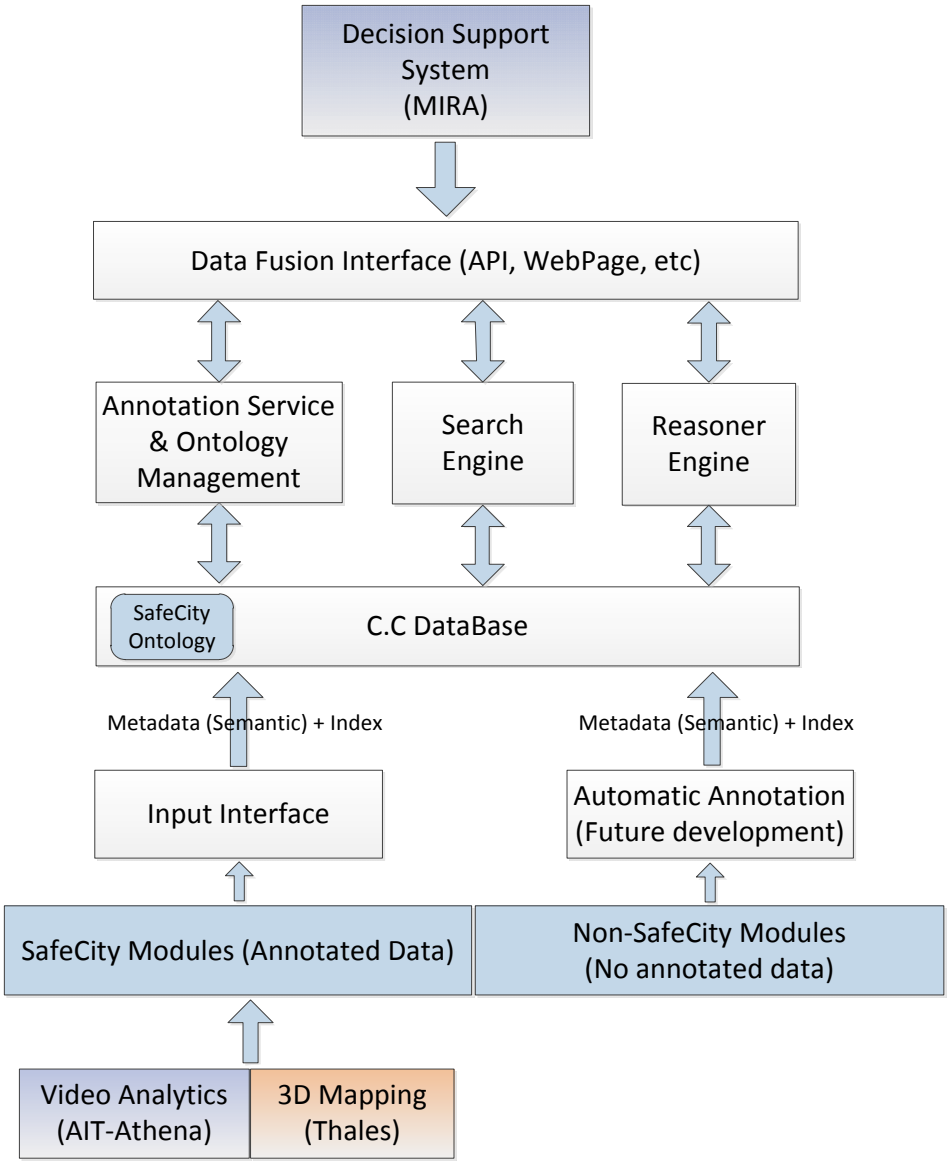


Figure 9 HIB application features

6.3 Requirements

Requirements	Generic Expression	Expression of requirements within the scope of the 1st WP4 trials
Ontology definition Requirement	In order to perform data fusion we need define an Ontology: • Ontology language (OWL, OWL2) • Ontology editor (Protegé)	In order to perform data fusion we need define an Ontology: • Ontology language (OWL, OWL2) • Ontology editor (Protegé)
Storage requirements	Assumptions: 100 to 5 000 events per	Assumptions: 100 events per second

(Only for metadata, not data itself like for example video)	second. • Space for each event can vary, suppose 1K (mean). • 5MB second • 300MB minute • 18000MB Hour • 432 GB / Day • 157 TB / Year	• Space for each event can vary, suppose 1KB (mean). • 100KB second • 6MB minute • 360MB Hour • 8,64 GB / Day • 3,15 TB/ Year
Reasoner engine	To infer new knowledge a Reasoner Engine is required. • Racer • FacT • Pellet • Hermit	Optional
Search engine	To allow queries a Search Engine is required. • SPARQL	To allow queries a Search Engine is required. • SPARQL
Computational requirements	The above requirements going to make intensive use of computational resources, especially search and reasoner engines. In order to satisfy these requirements, some enablers like cloud computing and big data processing could be used.	Optional

Table 8 Requirements for the Data Fusion application

6.4 Identification of useful GE/features proposed by FI-WARE [1]

FI-WARE ref.	GE title	SafeCity Comments	SafeCity Priority
3.2.1	IaaS DataCenter Resource Management	Virtual Machine (VM) hosting capabilities, as well as management of the corresponding resources within the DataCenter that hosts a particular FI-WARE Cloud Instance are mandatory.	MUST
3.2.2	IaaS Service Management	A top layer of IaaS Resource Manager to deal	SHOULD

		with definition of virtual resources specifying its needs to run an application, the relation between virtual resources, etc. should be useful.	
3.2.3	PaaS Management	Not necessary for SafeCity, due the underlying infrastructure of virtual resources probably will be known.	WONT
3.2.4	Object Storage	Not clear description of objectives' enabler.	WONT
3.2.5	Cloud Edge		COULD
3.2.6	Monitoring	Exploitation of SafeCity will probably require measurements of infrastructures	SHOULD
3.2.7	Resource Metering and Accounting	TBD	
4.2.1	Big Data Processing	Vary useful for Search Engine, Reasoning Engine.	MUST
4.2.2	Complex Event Processing	Could be useful for Alerting citizen's capabilities	MUST
4.2.3	Multimedia analysis to gather multimedia meta-data	Useful for Data Fusion module for annotation of multimedia legacy databases or external to SafeCity multimedia providers. Could be also very useful for other SafeCity applications such as Video Analytics	MUST
4.2.4	Pre-processing of meta-data during/after gathering	Useful for Data Fusion module for annotation of legacy databases or external to SafeCity data providers. Could be also useful for other SafeCity applications.	MUST
4.2.5	Preprocessing of unstructured data during/after gathering	Could it be adapted for SafeCity intelligent and sensor extensive processing?	WONT
4.2.6	Localization Platform	Provide an enhanced localization service is mandatory in SafeCity, due GPS not offer cover in some places like buildings, etc. Would be one of the metadata components.	MUST
4.2.7	Query-access	Useful in multimedia data will be stored into legacy or external databases.	COULD
4.2.8	Publish/Subscribe Broker	Useful for developing API for Data Fusion and other SafeCity modules. Could be useful for alerting citizens.	MUST
4.2.9	Semantic Annotation enabler	Useful for manual annotation / enriching of SafeCity Data	MUST

4.2.10	Semantic Application Support enabler	Useful for DataFusion module, some modules' enabler could be optional and therefore don't be utilized by DataFusion module.	MUST
4.3.1	Social Network Analysis	Could be useful to integrate social networks information into SafeCity Data Fusion module	COULD
4.3.2	Mobility Analysis	Could be useful for alerting citizen's capabilities	COULD
4.3.3	Real-time recommendations	Could be useful for alerting citizen's capabilities. We can consider an alert like a subtype of recommendation.	COULD
4.3.4	Behavioural and Web profiling	Could be useful to integrate social networks information into SafeCity Data Fusion module in a more advanced version.	COULD
4.3.5	Opinion mining	Could be useful for SafeCity Data Fusion module in a more advanced version.	COULD
5.2.**1**	USDL Service Descriptions	Not useful for our application	COULD
5.2.**2**	Model Repository	Not useful for our application	COULD
5.2.**3**	Service Registry	Could be useful for implementing APIs for SafeCity modules	COULD
5.2.**4**	Marketplace	Not useful for our application	WONT
5.2.**5**	Business Models & Elements Provisioning System	Not useful for our application	WONT
5.2.**6**	Revenue Settlement & Sharing System	Not useful for our application	WONT
5.2.**7**	SLA Management	Not useful for our application	SHOULD
5.3.3	Composition editor	Composition services are not useful for our application	WONT
5.3.4	Application mashup editor	Composition services are not useful for our application	WONT
5.3.5	Service composition editor	Composition services are not useful for our application	COULD
5.3.6	Execution engine	Composition services are not useful for our application	COULD
5.3.7	Mashup execution engine	Composition services are not useful for our application	COULD

5.3.8	Service composition engine	Composition services are not useful for our application	COULD
5.3.9	Service orchestration engine	Composition services are not useful for our application	COULD
5.3.10	Aggregator repository	Composition services are not useful for our application	COULD
5.4.1	Data Mediation	Mediator could be useful to guarantee interoperability between services SafeCity	SHOULD
5.4.2	Protocol Mediation	Mediator could be useful to guarantee interoperability between services SafeCity	SHOULD
5.4.3	Process Mediation	Mediator could be useful to guarantee interoperability between services SafeCity	SHOULD
5.5.1	Multi-channel/Multi-device Access System	Not useful for our application.	WONT
6.2.1	IoT Communications	To integrate underlying protocols used by various devices and gateways.	MUST
6.2.2	IoT Resources Management	Not useful for our application	WONT
6.2.3	IoT Data handling	Not useful for our application	WONT
6.2.4	IoT Process Automation	Not useful for our application	WONT
7.2.1	Connected Devices Interfacing (CDI)	Out scope provide a unified API for app developers	WONT
7.2.2	Cloud Edge	A custom made Cloud Edge Device should be developed for SafeCity, very different from the one targeted in FI-WARE (Home Scope).	SHOULD
7.2.3	Network Information and Control (NetIC)	An abstraction of the physical network resources, as well as the capability to control them are recommended	SHOULD
7.2.4	Service, Capability, Connectivity, and Control (S3C)	Not necessary for our application.	WONT
8.2.1	Security monitoring	Useful for the implementation of the information security system.	MUST
8.2.2	Identity Management	Useful for the implementation of the information security system.	MUST

8.2.3	PrimeLife Policy Language (PPL) Engine	Useful for the implementation of the information security system.	SHOULD
8.2.4	Identity Mixer (IdeMix)	Useful for the implementation of the information security system.	SHOULD
8.2.5	Context-based security and compliance	Useful for the implementation of the information security system.	SHOULD
8.2.6	Optional Security Service Enabler	Useful for the implementation of the information security system.	SHOULD

6.5 Entries for the FI-PPP backlog

See Cf. Annex : feature backlog entries to check the detail specifications regarding this applications.

6.6 Ask for new features to FI-WARE

This section includes petitions to Fi-Ware, in order to make easier his possible inclusion in this document, the following enablers will be described using the same format used by [1].

6.6.1 Manual annotations

Despite numerous advances in Artificial Intelligence and Machine Learning, today there are few systems that use these techniques in an intensive manner, and those that use some kind of Artificial Intelligence all adopted decision still under human supervision.

This enabler will provide functionalities for add meta-information to audiovisual content, according to a defined Ontology, providing all required features allowing its visualization, modification and addition of meta-information independently of their format (audio, video, text, etc.). Therefore this enabler could be included at sections “The Semantic Annotation Enabler (4.2.9)” or “Semantic Application Support enabler (4.2.10)” of FIWARE High-level Description [1].

These meta-information should be added by expert users or trained user (operators), allowing to enrich knowledge in a collaborative manner. For example, in video analytics can usefully offer a useable interface that will allow performing manual annotations, normally the manual annotation is motivated because the Artificial intelligence algorithm can’t detect a concrete event or situation, e.g. it’s too complicated detect if a concretely building is a bank or not, therefore this expertise knowledge should be provided by expertise users. This drawback can be motivated by different reasons; In the first one, the machine learning or Artificial intelligence algorithm can’t detect a concrete event or situation, whereas a trained operator can do it, in this case the trained operator collaborates with Machine Learning trying minimize their drawbacks or limitations. In the second one the operator collaborates with Machine Learning tagging new situations and updating the previously defined knowledge. Moreover due one type of Machine Learning algorithms are supervised, the manually annotated audiovisual content can be used like training set.

These manuals annotations are quite important, due the knowledge of whole system is increased, allowing performs perform queries showing matches elements and relationships between them using the Search Engine.

6.6.2 Priority communications

Target Usage

The Priority Communications Enabler will provide to FI-WARE the necessary mechanisms to optimally prioritize both voice and data communications since they are mandatory in order to assist Smart Cities. This enabler can also make use of the following GEs defined by FI-WARE:

- Network Information and Control (NetIC).
- Service, Capability, Connectivity, and Control (S3C).

Since these GEs do not address priority communications in a holistic way a new Priority Communications Enabler has to be defined focusing on two aspects: prioritization in access networks, both wireline and wireless networks, and prioritization in transport and core networks. Furthermore, mechanisms to properly manage the priority levels must be also addressed.

The need to include the Priority Communications Enabler is motivated by certain circumstances:

- Safety and critical situations, where the ability to transmit priority voice and data and know the IoT state is critical for Public Safety Agencies;
- Connectivity for mass public and companies, where the ability to discriminate voice and data according to certain policies (i.e. amount of data transmitted, type of services, etc…) could be hugely beneficial.

A fundamental challenge for the implementation of Priority Communications Enabler is that the priority mechanisms have to be considered for each different access network, as for example, LTE and UMTS for wireless networks or DSL and optical fiber networks for wireline networks; and also, in the transport and core networks. Furthermore, it must be taken into account that the implementation must be totally justified because of network neutrality concept.

Description

The Priority Communications Enabler comes to mitigate these challenges of the access and transport and core networks by offering an extended set of mechanisms that control and manage voice and data priority communications. These mechanisms implement the prioritization in access networks through correct access policies and the prioritization in transport and core networks by means of Deep Packet Inspection or Differentiated Services.

The first ones are applicable in most access networks. For example, for mobile access networks like GERAN (GSM, GPRS, EDGE), UMTS or LTE, two policies are needed: Call Admission Control Mechanism (CAC) and Congestion Control. These policies can be implemented through two functional entities: Radio Resource Manager (RRM) and Common Radio Resource Manager (CRRM). For fixed access networks like DSL or cable access networks, Multiprotocol Label Switching can be needed.

The second ones (prioritization mechanisms in transport and core networks) can be implemented through Deep Packet Inspection techniques. These inspections are realized tagging packets, and this tagging can occur in several places: at the network access points (accordingly to previously defined

policies), in other parts of the networks (taking into account congestion, network availability, etc.) and mostly in layers 2 and 3 of OSI.

6.6.3 Sensor edge

Other issue treated by [1] with a particular approach are Cloud Edge, this enabler allows user to deal with speed gap between LAN and ADSL networks, serving like proxy between user and the cloud. A similarly enabler can be useful for Smart Cities called “Sensor Edge”. Firstly this enabler could be useful to deal with the speed gap between sensor-gateway connection and gateway-command-centers connection; moreover this enabler could provide other features like data pre-processing or automated annotations.

This enabler can include different features, standardization of output video streams, automated annotations, etc. Since dealing with different providers and not being able to define at this point additional future developments in sensor technology, it is difficult to force a standardization model, yet more easy and effective to introduce 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 Ontology required.

Other feature performed by this enabler could be Machine learning algorithm adapted to a particular environment, since sensors connected to the same Sensor Edge are located at the same locations (same street). This approach helps the robustness, scalability and adaptability of the system. The following figure shows a schema of this enabler.

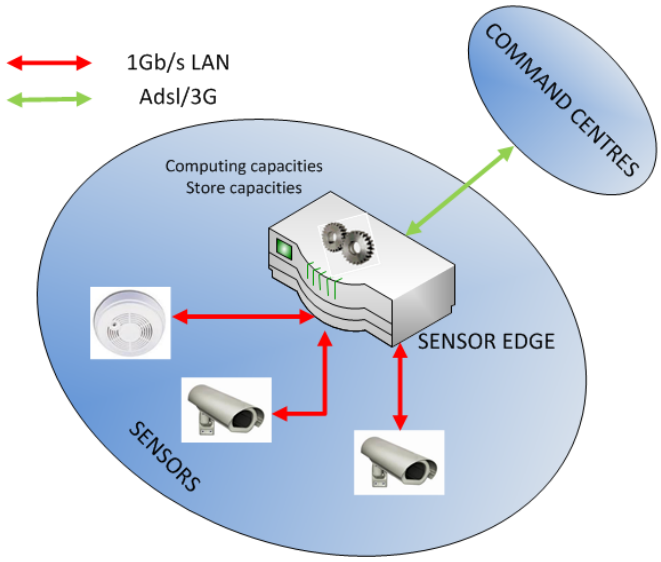


Figure 10 Model of sensor edge

6.7 ***Other***

Although FIWARE describes two enablers related with Semantics, Semantic Annotation (4.2.9) and Semantic Application Support (4.2.10) could be interesting complete these descriptions, providing an

enriched description. E.g. could be interesting include the Semantic Web Stack defined by World Wide Web Consortium (W3C), including a short description of each level.

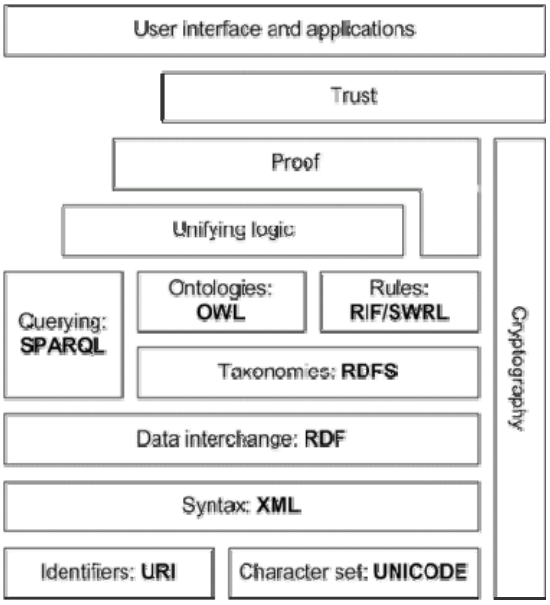


Figure 11 Semantic Web Stack defined by W3C

7. Application 6 "Communication Security" Features and Requirements

7.1 Short description

Wireless networks are based on a different set of assumptions and tradeoffs, requiring new thinking about the communication infrastructure. Especially, in the case of distributed sensor networking which is characterized by limited resources, immense scale of deployment and high level of heterogeneity, new architectures come into play that require new solutions for information security. In the scenarios envisioned by SafeCity, deployed sensing devices *(i)* may be mobile, so existing security solutions that assume fixed topologies cannot be employed; *(ii)* may have limited computational power and energy, necessitating the use of alternative cryptographic techniques, and *(iii)* may be carried by people as well, thus introducing more sophisticated security and trust concerns, as well as, new adversarial threat models.

In this setting, the goal of the security agenda with respect to security of communications will be to consider mechanisms to achieve an appropriate level of security taking into account the wireless nature of sensor networks, the context of the transmitted data and the inherent heterogeneity of the system for *(i)* deployed sensing devices based on different hardware platforms, and *(ii)* both fixed sensors (e.g. sensors deployed in specific locations) and mobile ones (e.g. sensors deployed in cars that can detect alerting situations on the move).

It is important to note that this work will not cover the security aspects of the interplay between the Cloud Hosting proxy and the end-users (e.g., privilege policies, access control schemes, etc.) since this is beyond the scope of the Communication Security application. The enablers and components to be developed and demonstrated here are responsible *only* for securing the intermediate communication between deployed IoT devices, gateways and the cloud proxy where any transmitted data will be stored later on.

Security Requirements

The problem at hand is to secure communications by designing protocols that mitigate attacks and thwart deviations from the implemented protocols to the greatest possible extent. Different protocols have their own specifications. However, rather than providing an exhaustive enumeration of sought after properties per protocol and application, we identify a set of standalone requirements.

The identified security requirements include:

- *Confidentiality* for protecting information disclosure to unauthorized parties. This is achieved through *encryption* which renders information unintelligible to unauthorized entities. Cryptographic algorithms are used in an appropriate *mode of operation* for enhancing the secrecy of associated private keys. Encrypted information may be recovered again by the use of *decryption*.
- *Message authentication and integrity*, to protect against any alteration and allow the receiver of a message to corroborate the sender of the message through a set of credentials. The use of MACs and digital signatures can lead to the detection of both accidental and malicious modifications made by an active adversary.

- *Message non-repudiation* so that the sender of a message cannot deny having sent a message.

- *Entity authentication* so that a receiver is ensured that the sender generated a message *and* has evidence of the *aliveness* of the sender. An entity can establish a lively correspondence with another entity using data-origin authentication techniques.

- *Trust and Group policies*, to determine the assignment of distinct roles to different types of nodes and their allowed actions within the system. As part of the security management features, *authorization* establishes what each node is allowed to do in the network.

Objectives & Achievements

The security architecture will revolve around the notion of a *Security Manager* (see Section 7.2), a Communication Security Specific Enabler (SE) that encapsulates the security aspects of the applications and enforces the desired communication security policies. It will be responsible for protecting network communications by defining the set of cryptographic transformations that have to be performed on the messages sent over the network. Overall, the Security Manager SE shall pervade the SafeCity project with a focus on *data access* and *communication* security. Security measures shall prevent threats like eavesdropping, integrity violations, masquerading, etc. through the use or proper encryption and authentication methods.

The concept and objectives of the Security Manager SE are to create a framework that can be integrated in any deployed IoT device/gateway and will allow the secure communication between participating entities. An overview of the areas that are covered by this specific enabler includes the following:

1. Security settings configuration (e.g., key management, cipher suite negotiation, etc.) and entity authentication between deployed sensing devices and gateways. This will lead to the establishment of secure communication channels.

2. Secure data handling (e.g., encryption/decryption, message authentication, integrity, etc.) of all measured/transmitted data depending on their context (e.g., support of various security levels).

3. Trust relationship schemes for determining deployed node profiles that include their allowed set of actions and the trustworthiness of the measured data/events.

In addition to the above, the mechanisms involved must be scalable and adaptable to the context of communications aiming at preserving energy and supporting the end-user while at the same time ensuring the security of transactions.

7.2 Features identification

This section is to provide documentation for the *Communication Security* (*CommSec*) application features and enablers, to be implemented, in order to provide the Public Safety smart capabilities (SafeCity). It includes:

1. System features and enablers (defined as CommSec Specific Enablers) to be implemented during development.

2. FI-WARE GEs and interface requirements that must be fulfilled by the underlying core platform.

7.2.1 Security Manager (SM) Specific Enabler

The security framework includes a cross-layer **Security Manager SE**, which controls all issues related to secure data transmission and establishment of a device trust relationship scheme at different levels of the SafeCity protocol stack. It enables the secure exchange of all network traffic regardless of sensor hardware and communication protocol heterogeneity, value range, precision or unit. *Operationally, this enabler will intercept messages that are transmitted through the (already established) network and apply the cryptographic transformations specified by the incorporated protocols.* Thus, through a *transparent* process (to the hosting IoT device/gateway), all outgoing traffic is encrypted (before transmission) and decrypted upon reception and before processing. Overall, the Security Manager is the central part of the system architecture and allows for adaptability in the applied security services, in order to map them with the security needs of each communication.

The SM enabler communicates internally with the FI-WARE. <Security Monitoring> GE; it tries to provide better feedback on detecting any ongoing intrusion attempt that can lead to an unauthorized access or alteration of the system's functionality. It uses intrusion detection monitoring to check network traffic and correlates all this information to create situational awareness reports that can pinpoint anomalies. Appropriate mitigation responses, based on specific attack patterns and events involved in an attack can be taken when necessary. The SM tries to use FiWARE mechanisms such as:

- **Monitoring for security effectiveness**: Get reports from FI-WARE Security Monitoring GE that show how well any security mechanism is working.
- **Monitoring vulnerabilities**: Use scanning on a regular basis to check for weaknesses.
- **Monitoring for changes in security configurations**.

To simplify configuration and enable pluggability, the Security Manager functionalities rely on the existence of three Specific Enablers (Figure 7.1) responsible for a certain system aspect: *Settings Configuration*, *Data Handling*, and *Trust Management*. These enablers, in turn, are composed of multiple components, each handling a specific task. This highly modular implementation mostly acts as a lightweight "*container*", delegating almost all behavior to the nested sub-enablers. The SEs will develop interfaces and interoperable mechanisms to support the above-mentioned secure communication between distributed things and devices/gateways in cooperation with various underlying FI-WARE enablers (Figure 7.1). This interaction will be enabled by provided agents to be integrated in all networking devices. The described SEs will also take into consideration the resource-constrained nature of sensing devices and will adopt lightweight cryptographic techniques. An abstract list of their (altogether) provided functionalities includes:

- **Cryptographic protocols abstraction**: A mechanism to enable the support of different security policy sets (e.g., cipher suites, cryptographic protocols, etc.) according to the application security needs. For instance, a "*strong*" security level parameter value will lead to the use of more sophisticated cryptographic techniques.

- **Authentication & Authorization**: Identification and verification, through a set of credentials, of the claimed identity of a communicating party. This is followed by an examination of the set of actions that this party can perform.
- **Data Processing**: Data compression, encryption using the produced encryption/decryption keys, integrity checks, etc.
- **Security Handling**: Dynamic negotiation and update of all cryptographic primitives.
- **Secure Session & Cache Management**: Configuration and management of any secure connection between distributed communicating things and devices/gateways.
- **Subject Trust Level Creation**: Development of a mechanism for setting and maintaining the trust level of each deployed IoT device depending on its location and area of events. This will also determine the significance of its measured data (can also be used to support *secure node addition*).

In what follows we will give a brief overview of each one of the Security Specific Enablers along with their *interaction* with any FI-WARE Generic Enablers. More detailed description and visualization of these SEs will be provided in subsequent versions of this deliverable. Specific FI-WARE GEs have been identified through the corresponding "FI-WARE High-Level Description" document and, thus, their functionalities will not be explained here.

7.2.1.1 Settings Configuration Specific Enabler

The **Settings Configuration (SC) SE** provides local computer and group policy-based configuration and analysis of security settings. This security configuration engine also supports the creation of security policy files. Based on context information provided by middleware services such as service discovery, node discovery, location positioning, etc., it performs adaptive and context-aware management for the security services. It configures the components of all other security SEs and establishes the connection to the cryptographic support module of *Data Handling*. To cope with different situations, the Settings Configuration maintains different policy sets according to the security needs, the device capabilities, the service and the user preferences. Policies can enable or disable some of the components or adjust their configuration, for example, to enhance or relax the parameters for secure communications.

The Settings Configuration SE will rely on inputs coming from the *Context based Security & Compliance* GEs of the underlying core platform. Basically, the required level of security (e.g., low, medium or high) will be provided by the FI-WARE. <Context-based Sec & Cmpl> GE and will be determined based on the context of data to be transmitted by a requested application. For instance, in crisis management scenarios where the significance and sensibility of produced/communicated data/events is high, the SC enabler will configure the corresponding security primitives to be used by the Data Handling SE during encryption, decryption, and/or transmission. Advanced cipher suites, "stronger" encryption/decryption keys, sophisticated cryptographic techniques, etc. will be used appropriately. Overall, the SC SE will create profiles and well defined interfaces for all supported security enablers/levels; however, they will be instantiated only when their use is required by certain applications.

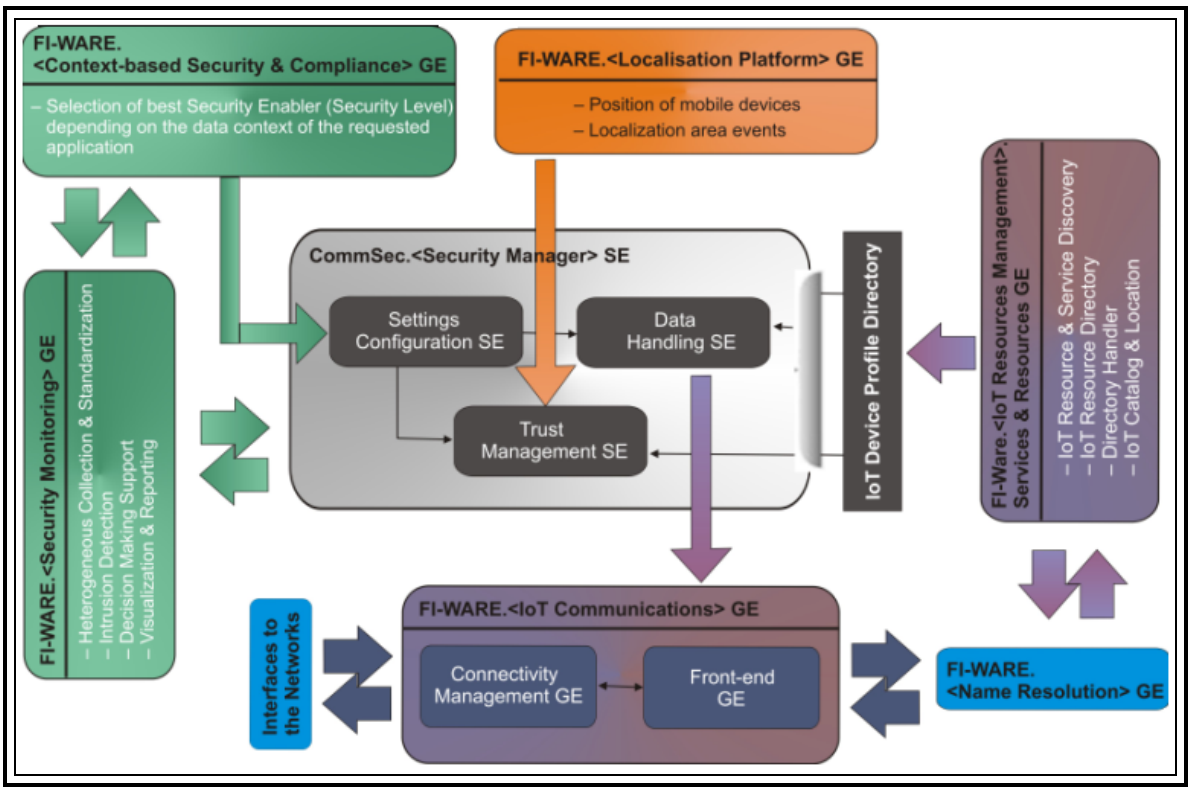


Figure 7.1 Architecture of CommSec Security Manager Enabler along with its 3 internal Specific Enablers (SEs); interaction flow with all necessary FI-WARE GEs is also depicted

Critical Attributes of Settings Configuration specific enabler

- Configuration of all credentials (certificates and key pairs) to be used by any authentication and encryption/decryption service.
- Support of a variety of security protocols based on context information provided by the FI-WARE Context-based Security & Compliance GE.
- Group policy-based configuration and analysis of security settings.

7.2.1.2 Data Handling Specific Enabler

The **Data Handling (DH) SE** deals with the secure exchange of information between networking IoT devices and gateways. Secure data handling is important in ensuring the integrity of transmitted data since it addresses concerns related to confidentiality, security, and preservation/retention of produced data. It provides resources pertaining to confidential data processing and transmission through authenticated message exchange. Its complexity lies in the encryption/decryption functions that will be used. These can vary depending on the security policy provided by the SC enabler such as:

- Utilization of advanced encryption techniques using appropriate bit key lengths and a variety of block ciphers, etc.
- Periodic refreshing of session keys depending on context and volume of communicating data and duration of operation.
- Utilization of Message Authentication (MAC) and/or digital signatures, etc.

The information exchange model shall be based on the concept of transmitting data through a secure established communication channel. Session keys, cryptographic techniques to be used and loaded cipher suites will be configured by the SC enabler before transmission. All encrypted data collections along with their metadata are forwarded to the FI_WARE. <Connectivity Management> &<Front-end> GEs for actual transmission. The use of these enablers ensures the successful communication of a broad range of different hardware *devices* regardless of their network status (static or mobile). The heterogeneous nature of sensor networks and embedded systems requires a flexible and interoperable solution to enable seamless interaction between high-level services and underlying deployed networks. As a consequence, the Front-End GE specifies a communication abstraction layer in order to integrate different underlying protocols used by all incorporated devices/gateways.

Critical Attributes of data Handling specific enabler

- Implementation of all necessary encryption/decryption and compression procedures to be performed on any data ready for transmission.
- Creation of the appropriate message stream to carry the processed data.
- Message stream processing (MACs, digital signatures, etc) for ensuring message authentication and integrity.

7.2.1.3 Trust Management Specific Enabler

The **Trust Management (TM) SE** is responsible for establishing trust relationships and managing access lists and security profiles when a new node joins the network or for subscription to new services. Trust plays an important role in IoT applications where the surrounding environment varies. The mechanisms introduced in this enabler specify, evaluate, establish, and ensure the trust relationships among IoT devices/gateways. In particular, its values are adaptively adjusted based on run-time trust assessment in order to reflect real system context and situation. Such functionalities are required for nodes that will need to communicate with nodes different from those that they were initially configured to trust.

In scenarios, like many IoT environments, that support the mobility of any underlying heterogeneous devices, it is beneficial to be able to retrieve *mobile device positions* and *localization area events*. The knowledge of when and where an event was triggered and/or measured can be used for extracting whether the transmitted information is trustworthy or not. Such a classification of information may

define associated information protection requirements in terms of restricting the acceptance and circulation of produced data. Based on this kind of location information, provided by the FI-WARE. <Localization Platform> GE, the TM SE may provide functionalities such as:

- **Control Stratification:** Assure that an entity handling, accessing and/or producing information as part of an operation process has the required privileges. The more sensitive the information is, the higher the requirement for the authentication result must be in order to be trusted.
- **Impact Sensitivity:** Determine the significance and trustworthiness of data/events that are produced by a specific entity. High impact sensitivity denotes trustworthy entities.

Critical Attributes of Trust Management specific enabler

- Specification, evaluation, establishment, and assurance of trust relationships among IoT devices and gateways.
- Management of access and trust lists.
- Control stratification and impact sensitivity.

7.3 Requirements

Requirements	Generic Expression	Expression of requirements within the scope of the 1st WP4 trials
Clock and localization-functions	For many applications, it is important to know when and where something was measured and/or happened. This requires the use of clock synchronization mechanisms. In networks with mobile nodes it must be possible to localize a node relative to other nodes	Optional
Requirements regarding Quality-of-Service	Networked control requires that QoS parameters can be monitored and possibly also controlled. Examples of requirements are: guaranteed end-to-end latency, bandwidth, network connectivity, etc.	Guaranteed bandwidth and network connectivity for the use of video cameras and mobile sensors
Mobility	The support of mobility of different parts of the network becomes an increasingly	The concept of MANETs seems the

	important requirement in many scenarios. The solutions can be structured in the following categories: • Host Mobility, i.e., when a mobile host dynamically changes its point of attachment to a fixed backbone, • Network Mobility, i.e., when a network in motion dynamically changes its point of attachment to a fixed backbone, and • Mobile Ad hoc Networks, i.e., when the backbone topology itself consists of mobile routers and consequently is dynamically changing.	most applicable to SafeCity trials
Heterogeneity and network re-configurability	Heterogeneity can come in many flavors – heterogeneous networks, different radio solutions, multitude of processor technologies. Network re-configurability is concerned with the overall network state and how to handle network dynamics (mobility, addressing and naming). The requirement on mobility in particular affects the routing and addressing mechanisms in the network.	Requirements for mobility, naming and addressing of nodes. Heterogeneity of network and hardware must be provided to some extend by appropriate middleware.
Re-configurability (cont.)	To simplify implementation and to support dynamic applications where the tasks change at run-time it should be possible to download program code and issue control commands or send programs over the network.	Optional
Automatic discovery of sensors/actuators connected	A service discovery mechanism	Optional.
Optimization of resources	Sensor networks, in particular, are often battery powered but are still assumed to have a long lifetime. Optimization of power resources affects routing and communicating protocols	Optional.
Security	The security solution should cover the communications between the nodes of sensor networks and between nodes and gateways to other networks. The architecture should also provide primitives necessary to meet security demands for various applications. These demands include but are not limited to	Security of communications must be provided to ensure confidentiality, integrity, etc. of data.

	data integrity, replay protection, data confidentiality, availability, authentication, access control, identity management, distribution and revocation of cryptographic keys, etc.	
Security interfaces to other layers or components	Security is handled in various modules and layers. For example the security manager must clearly interact with the networking module (using appropriate interfaces and handles) to protect the messages to be communicated. The middleware is considered as a module that is implemented on a node's hardware platform and that provides the application services. The middleware interacts with both the networking and security modules to help provide security at the application level.	Networking interfaces should be provided so that security is built on top of them. Middleware services should be provided at a lesser extent.

Table 7.1 Table of Requirements for Communication Security application

7.4 Identification of useful GE/features proposed by FI-WARE [1]

FI-WARE ref.	GE title	SafeCity Comments	SafeCity Priority
3.2.1	IaaS DataCenter Resource Management	This GE is independent from the *Communication Security Manager* to be implemented.	WONT
3.2.2	IaaS Service Management	This GE is independent from the *Communication Security Manager* to be implemented.	WONT
3.2.3	PaaS Management	This GE is independent from the *Communication Security Manager* to be implemented.	WONT
3.2.4	Object Storage	Such a GE provides an adequate storage mechanism for storing any produced data. It could be useful for providing interfaces and policies on how data/metadata will be stored (e.g., data structure format) *However, it is not directly coupled with the Communication security system.*	COULD/WONT
3.2.5	IaaS Cloud Edge	This GE is independent from the *Communication Security Manager* to be implemented.	WONT
3.2.6	Resource Monitoring	Such a GE could provide useful functionalities for the graceful degradation of the SafeCity project operation when some of the incorporated	

FI-WARE ref.	GE title	SafeCity Comments	SafeCity Priority
		Security GEs are not working properly. *This enabler, however, seems to be independent of the Communication security manager.*	COULD/WONT
3.2.7	Resource Metering and Accounting	Same as above	WONT
4.2.1	Publish/Subscribe Broker	This GE is independent from the *Communication Security Manager* to be implemented.	WONT
4.2.2	Complex Event Processing	Information security involves the secure *transmission* and *storage* of any produced data/events (regardless their amount). It is independent with how such data are processed for getting relevant insights. This is defined by the type of application run on the deployed sensors/actuators.	WONT
4.2.3	Big Data Analysis	N/A. Same as above	WONT
4.2.4	Multimedia analysis	Information security includes securing any data/event produced by the running application regardless its type (multimedia, text, etc.). Information content processing is independent with the project's security feature.	WONT
4.2.5	Unstructured data analysis	Information and metadata processing is independent with the project's security feature. Required processing of accompanied security metadata will be handled internally by the *Communication Security Manager*.	WONT
4.2.6	Meta-data Pre-processing	Same as above, this GE is independent from the *Information Security Manager* to be implemented.	WONT
4.2.7	Localization Platform	For many applications (especially in crisis management scenarios), it is important to know when and where something was measured and/or happened. Such information can be added as metadata by the *Communication security* system. This requires the use of a localization platform able to locate a node relative to other nodes.	SHOULD/COULD
4.2.8	Query Broker	How data, stored in the cloud, are retrieved by the end users is independent from the project's *Communication* security feature. Defined access	WONT

FI-WARE ref.	GE title	SafeCity Comments	SafeCity Priority
		and/or control policies will be responsible for such functionality.	
4.2.9	Semantic Annotation	Such a GE is independent from our *Communication security* system.	WONT
4.2.10	Semantic Application Support	Such a GE is independent from our *Communication security system*. However, representing data, to be transmitted and stored, through ontology objects can be proved helpful (in terms of storage capacity, security processing time and access permission definition) in future versions of the SafeCity project.	WONT
4.3.1	Social Network Analysis	In some applications, sensors may be placed in the hands of the users (e.g., use of mobile phones). In such cases, building the social profiles of both the individuals and communities can be used by our *Communication security* system for establishing *trust relationships* and managing access lists and security profiles when a new node joins the network or for subscription to new services. *However, it is not mandatory for the initial proof of concept.*	COULD/WONT
4.3.2	Mobility Analysis	Same as above, the analysis of such a GE can be used for extracting meaningful patterns of a user's behavior and establishing *trust relationships*. *However, it is not mandatory for the initial proof of concept.*	COULD/WONT
4.3.3	Real-time recommendations	N/A	WONT
4.3.4	Web behavior analysis for profiling	N/A	WONT
4.3.5	Opinion mining	N/A	WONT
5.2.1	USDL Service Descriptions	N/A	WONT
5.2.2	Repository	N/A	WONT
5.2.3	Registry	N/A	WONT

FI-WARE ref.	GE title	SafeCity Comments	SafeCity Priority
5.2.4	Marketplace	N/A	WONT
5.2.5	Business Models & Elements Provisioning System	N/A	WONT
5.2.6	Revenue Settlement & Sharing System	N/A	WONT
5.2.7	SLA Management	Such a QoS delivery system is mandatory especially in the case of crisis management scenarios. Examples of requirements are: guaranteed end-to-end latency, bandwidth, network connectivity, etc. *This enabler, however, seems to be independent of the Communication security manager.*	WONT
5.3.1	Composition editor	N/A	WONT
5.3.2	Mashup execution engine	N/A	WONT
5.3.3	Service orchestration engine	N/A	WONT
5.3.4	Service composition engine	N/A	WONT
5.4.1	Mediation	Information security includes securing any data/events that may be produced by various types of sensor hardware. Therefore, it is mandatory to have a flexible mechanism that supports such a sensor heterogeneity in terms of: • Data structure of transmitted/stored information. • Variety of underlying network protocols. *This functionality along with the next two basically describes the operation of IoT Communication GE which is adopted in our case (see 6.2.1).*	WONT
5.4.2	Protocol Mediation	Same as above. See 6.2.1	WONT
5.4.3	Process Mediation	Same as above. See 6.2.2	WONT

FI-WARE ref.	GE title	SafeCity Comments	SafeCity Priority
5.5.1	Multi-channel/Multi-device Access System	Such a GE can enhance the QoS provided by the *Communication security* system. *However, it is not mandatory for the initial proof of concept.*	WONT
6.2.1	IoT Communications	It is mandatory to have a flexible mechanism that supports sensor heterogeneity. Such a GE can provide generic access (through gateways, etc.) to every kind of deployed sensors regardless of the underlying hardware.	MUST
6.2.2	IoT Resources Management	The information security system's functionality is **independent** from any unified services for *utilizing* and *activating* deployed sensor functionalities and managing their properties. However, to support dynamic applications where the tasks change at run-time it should be possible to download program code and issue control commands or send programs over the network. This enabler (if exists) can be used by the Security manager to support heterogeneity.	MUST/SHOULD
6.2.3	IoT Data handling	Securing the raw data (accompanied by necessary security metadata) produced by any deployed sensor may result in big data rates requiring higher link bandwidths. Therefore, flexible data processing functions aiming to generate a smaller set of elaborated data **locally** can significantly improve the QoS of SafeCity. *This enabler, however, seems to be independent of the Communication Security manager.*	COULD/WONT
6.2.4	IoT Process Automation	The information security system's functionality is **independent** from any underlying process interactions which may include *asynchrony* and *concurrency*. However, since all intra - and inter – sensor process events must be captured adequately, such a GE can provide important functionalities for any upper layer applications.	WONT
7.2.1	Connected Devices Interfacing (CDI)	Same as above, such a GE can provide important functionalities for any upper layer applications. *However, it is not directly coupled with the information security system.*	WONT
7.2.2	Cloud Edge	Cf. 3.2.5	WONT

FI-WARE ref.	GE title	SafeCity Comments	SafeCity Priority
7.2.3	Network Information and Control (NetIC)	Transmitting, in a secure manner, any produced data/events require the knowledge of network status information concerning flow processing, routing, addressing, and resource management at flow and circuit level. *However, it is not directly coupled with the Communication security system.*	WONT
7.2.4	Service, Capability, Connectivity, and Control (S3C)	Such a GE is not mandatory for the core functionality of the information security system. However, it can provide useful services for building *access control* schemes in order to **monitor** possible violations of the network environment usage rules.	WONT
7.3.1	Identity and privacy management	Mandatory for the implementation of the *information security* system. However, we manage internally such **identity** and **access control** schemes.	WONT
8.2.1	Security monitoring	It is advisable to continuously collect and monitor raw data (from large-scale heterogeneous environments) in order to achieve the execution of services with desired security behavior and detection of potential attacks or non-authorized usage. Therefore, such an enabler is useful for the implementation of the *Communication security* system.	MUST
8.2.2	Identity Management	Cf. 7.3.1.	WONT
8.2.3	PrimeLife Policy Language (PPL) Engine	Such a GE may be used for configuring data access rights in order to safeguard private information of the system users; for example we may be interested in providing *anonymity* for the actions (messages and transactions) of the mobile users. *However, it is not mandatory for the initial proof of concept.*	WONT
8.2.4	Identity Mixer (IdeMix)	Same as above, in the context of secure communication we may be interested in providing *anonymity* for the actions of the mobile users. However, it doesn't seem to apply for the PoC scenarios.	WONT

FI-WARE ref.	GE title	SafeCity Comments	SafeCity Priority
8.2.5	Context-based security and compliance	Such a GE is mandatory for providing various levels of security depending on the importance of the application information context (especially for crisis management scenarios).	MUST
8.2.6	Optional Security Service Enabler	N/A	WONT

7.5 Entries for the FI-PPP backlog

Cf. Chapter 0 for detailed inputs and Chapter 13 for synthesis.

7.6 Ask for new features to FI-WARE

Although no new FI-WARE features are required, the enablers described in Section 7.2 could also be made part of FI-WARE if there is an overlap with other Use Case projects. Additionally, having a cleaner list of the Generic Enablers (and their functionalities) that will be provided by the FI-WARE core platform would be helpful.

8. Application 7 " Decision support" Features and Requirements

8.1 Short description

SafeCity project includes a Decision Support System (DSS) which is a knowledge based system that supports organizational decision-making activities. DSS serve the operators and planning levels of the system to take the appropriate actions, which may be rapidly changing and not easily specified in advance.

Purpose

The purpose of DSS module is to integrate Data Fusion module provided by Hi-Iberia with the User Interface module.

Functionality

The DSS module performs the following functionalities:

1. Get commands and messages from the above mentioned module
2. Dispatch commands and messages to the DataFusion and User Interface module
3. Get user input, decide what module should receive the data, compose the proper messages/commands
4. Based on the user input compose the right message / command in order to address the proper sensor or alerting device
5. Define automated responses to be delivered by the MIT Decision and Support System to the Data Fusion module

The core of DSS engine will be build up to support the Data Fusion module. In order to achieve this interface must be provided. A standard communication protocol will be specified and the command and message format will be developed. The module gets the input from the operators and feeds the DSS engine which processes the information and routes the commands and data to the appropriate module (Data Fusion module). All the alerts provided by the Data Fusion module are interpreted and the proper information is presented to the operator/decision maker.

DSS extension module – the deliverable will include detailed description of standard protocol used, format of messages and command, format of the alerts and operators commands.

Inputs

- Commands and Data provided by the Data Fusion application
- Operator input
- Dispatching rules

Outputs

- Alert data to be sent to the UI module
- Commands and data to Data Fusion application

Constraints

- All data must be well formatted (i.e. xml) and must comply with format description (xsd)

8.2 Features identification

8.2.1 DSS diagram

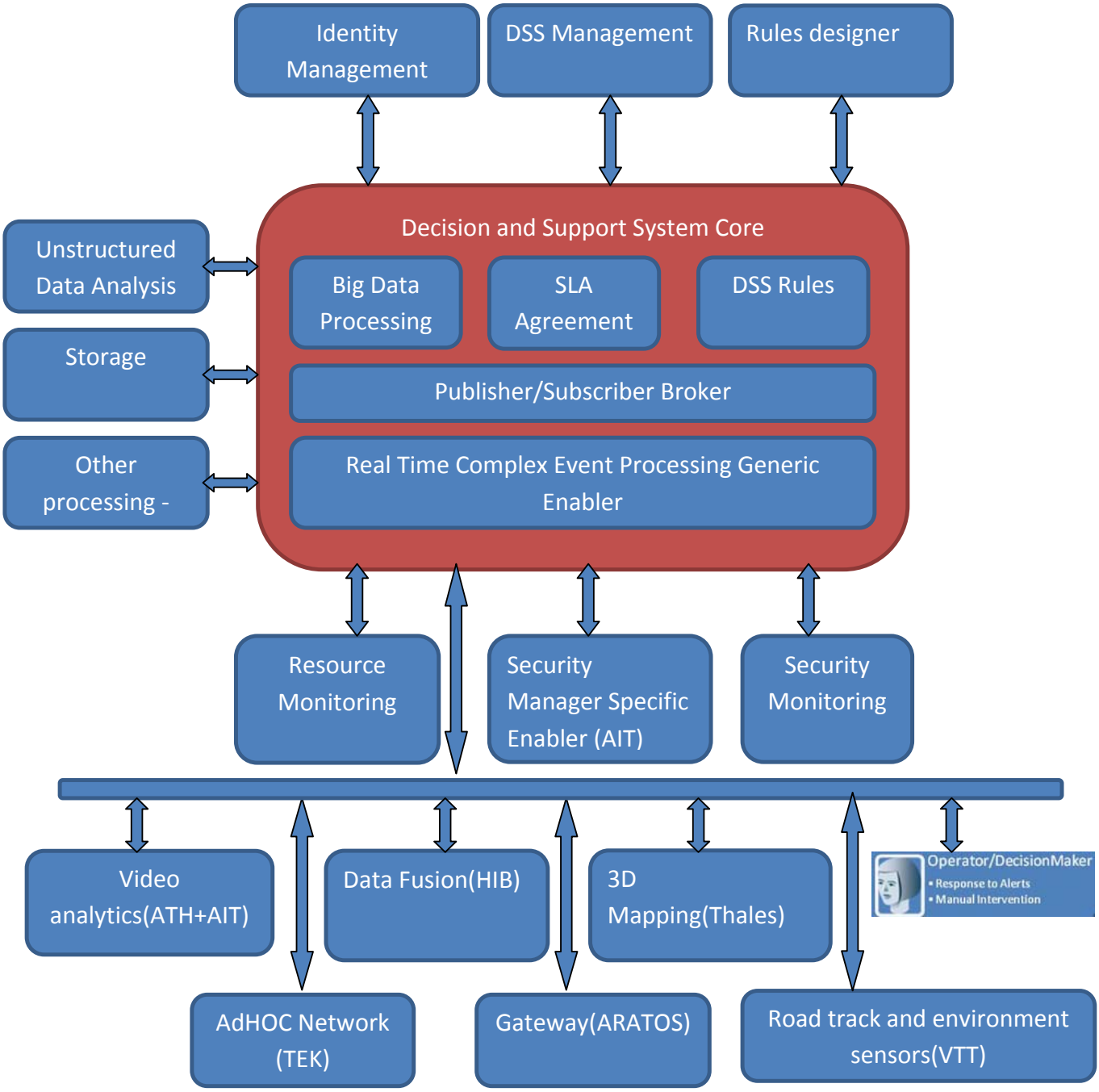


Figure 4 DSS application features

8.2.2 Required features

A DSS will make the connection between several applications and devices (Video Analytics, Data Fusion, 3D Mapping, AdHoc Network Nodes, Sensors, Actuators, User Interface) that are part of a CCC stack. Its purpose is to receive messages (especially from Fusion Engine, but not limited to), process them and respond to them according to the rules designed by the Rules Designer. The rules specified will allow the DSS to generate automated response.

The DSS has a module that is able to process a large quantity of messages and way to manage all publishers / subscribers. The distribution model for the messaging can be push or pull.

Due to the sensitive nature of the data processed by the DSS, it must provide its services guaranteeing various Key Performance Indicators (processing, communication latency, etc.).

The communication between different applications and sensors is encrypted. Mechanisms like authentication, verification, signing, encryption (symmetric and asymmetric), encoding and other cryptographic methods should be provided in order to increase security and privacy level. The identity of the partners involved should be known and permanently verified.

All events are stored in a database for later analysis.

A DSS application should be accompanied by a mechanism for resource metering and accounting and security monitoring.

8.2.3 Required GEs

Complex Event Processing, Publish/Subscriber Broker, Big Data Processing

8.2.4 Decision Support additional GEs

Unstructured Data Analysis, Monitoring, Resource Metering and Accounting, Security monitoring

Identity management, SLA Management

8.3 Identified Constraints/requirements

Requirements	Generic Expression	Expression of requirements within the scope of the 1st WP4 trials
Bandwidth requirements	Depending on the number and nature of message processed by DSS the bandwidth requirements can scale up to several Mbps. The system should be able to scale up and down network bandwidth effortlessly, without affecting latency.	For the demonstration purpose 1 Mbps should be enough.
Latency requirements	Due to the fact that the information contained in the messages processed by the DSS has a very strong time constraint, the latency should be as close as it gets to real time. In practice less than 100 ms latency is acceptable.	For the demonstration purpose a latency close to 100 ms is acceptable.
Privacy requirements	Sensible information contained in the messages must be protected from illegal access.	No need for the demo.
MetaData	All the messages processed by the DSS should be timestamped with the system clock in order to associate the decisions with data.	Optional.
Processing latency	Due to the sensitive nature of the information contained in DSS messages, a mechanism should be provided in order to minimize the processing latency, A mechanism to secure the processor bandwidth for the processing threads should be provided.	Optional.
Scaling processing power	The system should be able to scale up and down effortlessly. In case of events that generate big amounts of data, the system should be able to acquire more processing power without affecting the latency. The system should be able to run natively on more than one processor/machine.	Optional.
Security Requirements	Messages providers and consumers that work with the DSS must be authenticated before having access to DSS application. Access level to the DSS operation must be dynamically configurable.	Optional.

Clock provider	All the messages exchanged between applications should be time stamped allowing message correlation, performance assessment, distributed transaction coordination and reliable communication.	-

Table 2 Requirements for MIT application

8.4 Identification of useful GE/features proposed by FI-WARE [1]

FI-WARE ref.	GE title	SafeCity Comments	SafeCity Priority
3.2.1	IaaS DataCenter Resource Management	N\A (Is mandatory for every FI-WARE cloud instance)	SHOULD
3.2.2	IaaS Service Management	N\A	SHOULD
3.2.3	PaaS Management	N\A	SHOULD
3.2.4	Object Storage	N\A	SHOULD
3.2.5	Cloud Edge	N\A	WONT
3.2.6	Monitoring	This GE should be available for debugging, bottlenecks identification, etc.	SHOULD
3.2.7	Resource Metering and Accounting	Same as above	SHOULD
4.2.1	Publish/Subscribe Broker	This GE should provide publishers subscribers management.	MUST
4.2.2	Complex Event Processing	This GE should be available in order to allow DSS to process events generated by applications.	MUST
4.2.3	Big Data Analysis	Same as above.	MUST
4.2.4	Multimedia analysis	N\A	WONT
4.2.5	Unstructured data analysis	Could be a data source for DSS	COULD
4.2.6	Meta-data Pre-processing	Could be a data source for DSS	COULD
4.2.7	Localization Platform	Useful when sending messages to sensors/actuators that are located in a specific area.	SHOULD
4.2.8	Query Broker	N\A	WONT
4.2.9	Semantic Annotation	N\A	WONT

4.2.10	Semantic Application Support	N\A	WONT
4.3.1	Social Network Analysis	N\A	COULD/WONT
4.3.2	Mobility Analysis		COULD/WONT
4.3.3	Real-time recommendations	N/A	WONT
4.3.4	Web behavior analysis for profiling	N/A	WONT
4.3.5	Opinion mining	N/A	WONT
5.2.1	USDL Service Descriptions	N/A	WONT
5.2.2	Repository	N/A	WONT
5.2.3	Registry	N/A	WONT
5.2.4	Marketplace	N/A	WONT
5.2.5	Business Models & Elements Provisioning System	N/A	WONT
5.2.6	Revenue Settlement & Sharing System	N/A	WONT
5.2.7	SLA Management	This GE is mandatory for guaranteed processing latency, communication latency, bandwidth, network connectivity, etc.	MUST
5.3.1	Composition editor	N/A	WONT
5.3.2	Mashup execution engine	N/A	WONT
5.3.3	Service orchestration engine	N/A	WONT
5.3.4	Service composition engine	N/A	WONT
5.4.1	Mediation	N\A	WONT
5.4.2	Protocol Mediation	N\A	WONT
5.4.3	Process Mediation	N\A	WONT
5.5.1	Multi-channel/Multi-device Access System	N\A	WONT
6.2.1	IoT Communications	Should be available for communicating with sensors/actuators.	MUST
6.2.2	IoT Resources Management	N\A	WONT

6.2.3	IoT Data handling	N\A	WONT
6.2.4	IoT Process Automation	N\A	WONT
7.2.1	Connected Devices Interfacing (CDI)	N\A	WONT
7.2.2	Cloud Edge	Cf. 3.2.5	WONT
7.2.3	Network Information and Control (NetIC)	N\A	WONT
7.2.4	Service, Capability, Connectivity, and Control (S3C)	N\A	WONT
7.3.1	Identity and privacy management	N\A	WONT
8.2.1	Security monitoring	Useful for monitoring threats.	MUST
8.2.2	Identity Management	Cf. 7.3.1.	WONT
8.2.3	PrimeLife Policy Language (PPL) Engine	N\A	WONT
8.2.4	Identity Mixer (IdeMix)	N\A	WONT
8.2.5	Context-based security and compliance	N\A	WONT
8.2.6	Optional Security Service Enabler	N\A	WONT

8.4 Entries for the FI-PPP backlog

Cf. Chapter 0 for detailed inputs and Chapter 13 for synthesis.

9. Application 8 "Road track and environment sensors" Features and Requirements

9.1 Short description

The sensing applications for road track and environment can be divided for two different purposes. The first is to monitor the *weather conditions* occurring specially when certain threshold values (e.g., near zero Celsius degrees) are met. Additionally to temperatures (both air and the road), sensors can be used for identifying the strength of the wind, humidity, raining and snowing.

The second area of monitoring is *traffic flows and fluency.* This includes the amount of cars on the roads and cross-roads, average speeds, traffic congestions, illegal and dangerous parking, and incidents and accidents.

The sensors itself can include both fixed (road track, on the side of the road, fixed cameras, etc.) and mobile (on-board cameras, positioning sensors, acceleration sensors, etc. installed in vehicles or carried by humans (smart phones). Furthermore, the mobiles sensing systems could utilise for communication and gateway the mobile phone.

9.2 Features identification

The applications and services are based on the pre-processed and analysed information from the sensors. The service end users can be e.g. citizens, officials, or the Police.

The direct services for the citizens include (re)routing information for the trip, notification related to weather or incidents on the road. The officials can get information related to traffic during mass happenings. The police can extract license plate data and compare that to e.g. stolen vehicle data base.

The system must be based on nearly zero configuration of the installed devices and sensors, as well as easy to access services for the end users. Additionally, pre-processing and analysing the data needs to take place in real time, and in case of timed out data the information needs to be discarded.

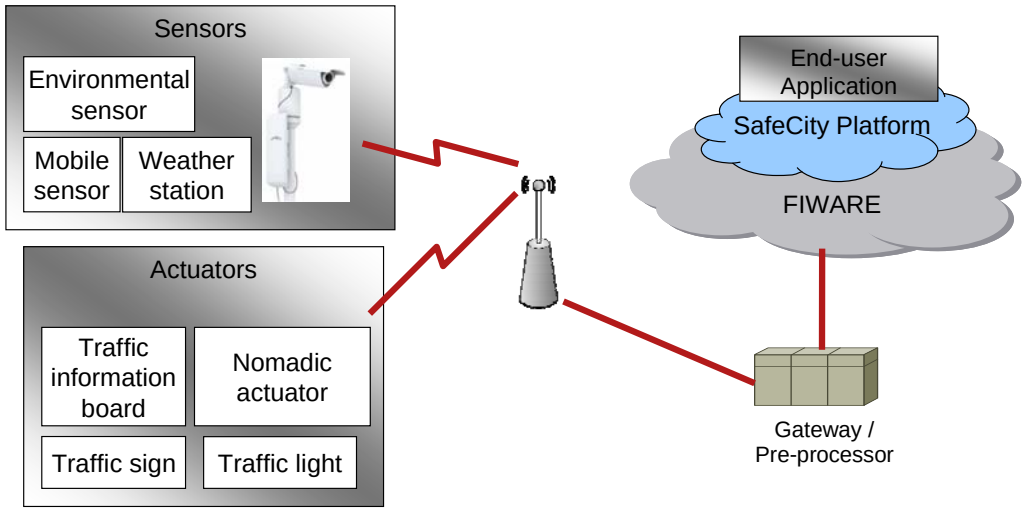


Figure 12 Features representation of the Road track and environment sensors application

Security, privacy, and trust must be maintained within the system in order to track down misbehaving devices and sensors, inhibit feeding of false information to the system, and prohibit extracting information related to citizen's privacy.

9.3 Identified constraints/requirements

Requirements	Generic Expression	Expression of requirements within the scope of the 1st WP4 trials
Sensor/actuator deployment	Devices need network connection, fixed or wireless. Bandwidth is device dependent (1 kbps – tens of Mbps). Electricity is also needed.	< 1Mbps bandwidth could be sufficient. Batteries can also be used when necessary.
Automatic Gateway discovery	Sensors and actuators must be able to discover gateway automatically.	Manual configuration.
Service and capability announcement	Sensors and gateways announce their existence and capabilities to gateway and other	Manual configuration.
Reconfiguration	There must be mechanism to reconfigure the devices remotely, also in a safe manner to prevent the device to become inoperative.	Only basic mechanisms needed.
Sensor clock synchronization	There must be mechanisms for continuous clock synchronization of sensors and actuators.	One-time clock synchronization during initialization phase is sufficient.
Localization	Location of IoTs must be known. Automated mechanisms should exist.	Manual configuration.
Sensor embedded storage	In case of networking problems local data storage must exists for lossless data communication.	Not required.
Sensor embedded data processing	Local data processing to decrease the amount of transported data and enable sensor to make decisions based on information gathered.	Not required.
Adaptive data transmission	Adapt to the varying network conditions to minimize data losses during transmission and prioritize important traffic.	Not required.
Pre-fault detection	Enable the sensor/actuator to be replaced or faults fixed before it becomes defunct e.g. battery wears out or	Not required.
Energy-efficiency	Data processing and transmissions must be minimized in order to gain energy-efficiency.	Not strictly necessary.
Physical protection	Prevent the theft or vandalism of devices. Installation to locations that are unreachable by any one or use proper physical protection/shielding.	Required.

Table 9 Requirements for VTT application

9.4 Identification of useful GE/features proposed by FI-WARE [1]

FI-WARE ref.	GE title	SafeCity Comments	SafeCity Priority
3.2.1	IaaS DataCenter Resource Management	Not useful for our application.	WONT
3.2.2	IaaS Service Management	Not useful for our application.	WONT
3.2.3	PaaS Management	Not useful for our application.	WONT
3.2.4	Object Storage	Not useful for our application.	WONT
3.2.5	Iaas Cloud-edge Resource Management	Maybe if Cloud Edge is used.	WONT/COULD
3.2.6	Resource monitoring	Not useful for our application.	WONT
4.2.1	Publish/Subscribe Broker	6.2.3 probably makes more sense. Smart phone could utilize this.	COULD
4.2.2	Complex Event Processing	6.2.3 probably makes more sense. Smart phone could utilize this.	COULD
4.2.3	Big Data Analysis	Most sensors are too constrained to do this. Smart phone could utilize this.	COULD
4.2.4	Multimedia analysis	Some camera might do this but mostly it's pre-processor or someone else doing this. Sensors and cameras are too constrained. Smart phone could utilize this.	COULD
4.2.5	Unstructured data analysis	Not useful for our application.	WONT
4.2.6	Meta-data Pre-processing	Pre-processing that could be done in cameras/sensors. Maybe IoT Data Handling suites better.	SHOULD
4.2.7	Localization Platform	Mandatory to localize sensors, cameras and actuators	MUST
4.2.8	Query Broker	Not useful for our application.	WONT
4.2.9	Semantic Annotation	Not useful for our application.	WONT
4.2.10	Semantic Application Support	Not useful for our application.	WONT
4.3.1	Social Network Analysis	Not useful for our application.	WONT
4.3.2	Mobility Analysis	Not useful for our application.	WONT
4.3.3	Real-time recommendations	Not useful for our application.	WONT
4.3.4	Web behaviour analysis for profiling	Not useful for our application.	WONT
4.3.5	Opinion mining	Not useful for our application.	WONT
5.2.1	USDL Service Descriptions	Not useful for our application.	WONT
5.2.2	Repository	Not useful for our application.	WONT
5.2.3	Registry	Not useful for our application.	WONT

FI-WARE ref.	GE title	SafeCity Comments	SafeCity Priority
5.2.4	Marketplace	Not useful for our application.	WONT
5.2.5	Business Models & Elements Provisioning System	Not useful for our application.	WONT
5.2.6	Revenue Settlement & Sharing System	Not useful for our application.	WONT
5.2.7	SLA Management	Is this applicable to sensors?	WONT/MUST
5.3.1	Composition editors	Not useful for our application.	WONT
5.3.2	Composition execution engines	Not useful for our application.	WONT
5.4.1	Mediation	To study when detailed	COULD
5.5.1	Multi-channel/Multi-device Access System	Not useful for our application.	WONT
6.2.1	IoT Communications	Mandatory for every IoT.	MUST
6.2.2	IoT Resources Management	Mandatory for every IoT.	MUST
6.2.3	IoT Data handling	Mandatory if sensors do some short of pre-processing and storage?	MUST/SHOULD
6.2.4	IoT Process Automation	To study when detailed	COULD
7.2.1	Connected Devices Interfacing (CDI)	Needed if user devices e.g. mobile phones act as a sensor or actuator.	COULD
7.2.2	Cloud Edge	Needed if user devices e.g. mobile phones act as a sensor or actuator.	COULD
7.2.3	Network Information and Control (NetIC)	Needed if user devices e.g. mobile phones act as a sensor or actuator.	COULD
7.2.4	Service, Capability, Connectivity, and Control (S3C)	Needed if user devices e.g. mobile phones act as a sensor or actuator.	COULD
8.2.1	Security monitoring	More like a FI-WARE instance related.	WONT
8.2.2	Identity Management	Maybe more related to end-users than in sensors. If end-user acts as a sensor identity management may be needed.	COULD
8.2.3	PrimeLife Policy Language (PPL) Engine	Not useful for our application.	WONT
8.2.4	Identity Mixer (IdeMix)	Maybe more related to end-users than in sensors. If end-user acts as a sensor enhanced privacy may be needed.	COULD
8.2.5	Context-based security and compliance	Not useful for our application.	WONT
8.2.6	Optional Security Service Enabler	Not useful for our application.	WONT

Table 10 Analysis of FI-WARE features/enablers for VTT application

9.5 Entries for the FI-PPP backlog

Cf. Chapter 0 for detailed inputs and Chapter 13 for synthesis.

9.6 Ask for new features to FI-WARE

10. Madrid Public Safety Scenarios Features and Requirements

11. Bucharest Public Safety Scenarios Features and Requirements

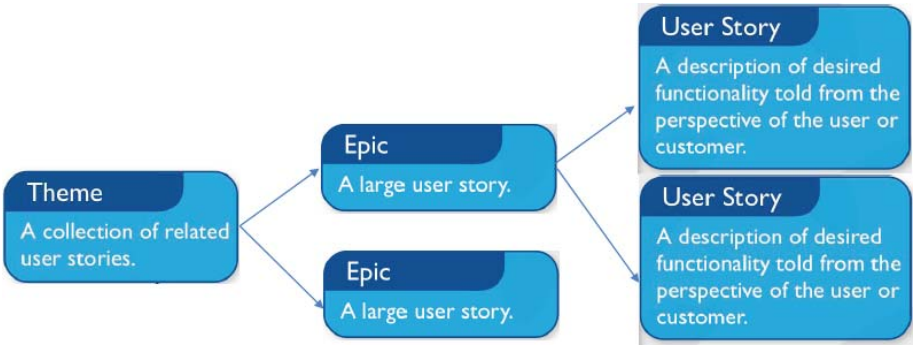
12. Stockholm Public Safety Scenarios Features and Requirements

13. Global feedback to FI-WARE

In this chapter, SafeCity features backlog is presented following instructions given in [2] and justified. Synthesis of Specific Requirements

13.1 Features backlog entries

In SafeCity Project the enablers requirement are part of the Specific requirement definition. Due to uncertainness about what will be provided by FI WARE platform in the specific requirement definition a set of Enablers taken from FI WARE HLD document [1] have been identified of enablers of interests and then a set of requirement has been put directly in the backlog entries format as defined by the Concord Architecture Board. In particular SafeCity has chosen to follow the Agile methodology for requirement specification considering the approach described in the following picture.



A Theme is a top-level objective that may span projects and products. At its most granular form, a Theme may be an Epic or more than one. Themes can be used at both Programme and Project Level to drive strategic alignment and communicate a clear direction.

An Epic is a large User story that can be broken into group of related User Stories. You would be unlikely to introduce an Epic into a Sprint without first breaking it down into its component User Stories.

A User story is an Independent, Negotiable, Valuable, Estimable, Small, Testable requirement ("INVEST"). Despite being Independent i.e. they have no direct dependencies with another requirement, User stories may be clustered into Epics when represented on a Product Roadmap.

Each application developers will then internally use its own development methods (not necessarily Agile) but the requirement to FI WARE are expressed following Agile methodology.

The SafeCity process to define backlog entries foresees a set of steps before the requirement is entered into FI WARE backlog entries tool. The process is defined in the following:

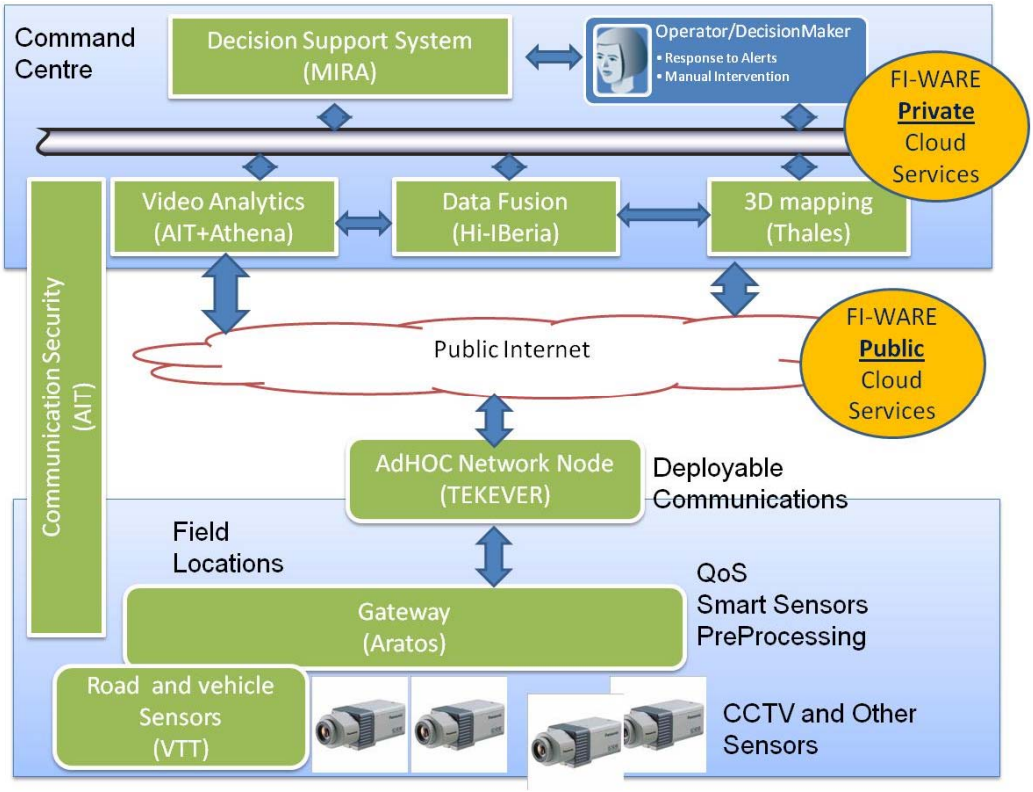
1. Each application developer would produce the backlog entries using the SafeCity private repository wiki and then, send email for comments to the other partners.
2. Technical partners would provide comments during one or two days, at most.
3. Then the agreed request to FI-WARE would be introduced by the application developer who produced it in the backlog entry tool from FI WARE.

4. Finally D3.1 would be updated accordingly by the partner responsible of (producing) the request.

This process of verification of backlog entries has been set up to avoid the introduction of overlapping backlog entries in the FI WARE tools. The phase 2 of the process in which every technical partners provide feedbacks to the backlog entries proposed is a very important steps and each application developer should do this check considering if its own requirement can be covered or are overlapping with the backlog entries proposed by the other application developers. Only after this check the application developer can insert the entry in the FI WARE backlog entry tool. After the input into the backlog entry a process of exchanging information with FI WARE experts is needed and expected and the tools defined by the Concord Architecture Board shall be used.

13.2 General comments and observations

Looking at the SafeCity general Architecture represented in the following figure we see that there are seven applications plus a transversal application related to Security that is very important in case of applications related to safety.



In the following there is the list of the Enablers needed by each application.

13.2.1 Video Analytics Enablers

The following enablers are needed: Multimedia Analysis GE, Semantic Application Support GE.

From Multimedia analysis GE it is expected: to provide the required video processing and analysis algorithms in order to visually perceive potential threat cases in camera monitored areas and to provide the capability to process and extract meaningful visual descriptors that uniquely characterize specific objects, events, patterns in video data.

The required functionality are:

- Visual facial descriptors extraction;
- Face detection
- Face recognition
- Background Scene registration
- Motion detection
- Moving Object segmentation
- Face modelling
- Orphan object detection
- Virtual line drawing
- Trespassing detection
- Moving Object Tracking
- Person Tracking

From Semantic Application Support GE it is expected: To create a definition of knowledge domain and multimedia ontologies, as well as metadata schemas within the context of the safety and security domains applied to video analytics, to manage video data (archived and streams) as well as metadata instances, to provide the ability to evolve the captured know-how (in the SafeCity ontology) based either on new suspicious behaviours observation, user inputs, or detection results (from other applications as well, coming from Data Fusion and DSS systems.

The required functionality are:

- Threat Ontology Definition;
- Metadata Generation
- Database Storage
- Reasoning Engine

The following features are expected from these enablers.

The following additional enablers maybe used (more information are necessary about the enablers) :

- IaaS Service Management;
- Object Storage
- Cloud Edge
- Pre-processing of meta-data during/after gathering
- Pre-processing of unstructured data during/after gathering
- Resource Monitoring
- Publish/Subscribe Broker
- Meta-data Pre-processing
- Query Broker
- Big Data Processing
- Complex Event Processing

- Identity and privacy management
- PrimeLife Policy Language (PPL)
- Semantic Annotation.

13.2.2 3D real time positioning Enablers

The following enablers are needed: Multimedia analysis, Big Data processing, Complex Event processing, IaaS service Management, Publish/subscribe broker

From Multimedia analysis: SpecificMetaDataHandling; This module should enable to annotate inputs and outputs of proprietary and business specific video analysis module. The API provided must enable to embed a "multimedia stream analysis" 3rd party (indeed, this function is business specific).

From Big Data processing: BigVideo; This module should allow the use of large bandwidth and large storage for video analysis purposes (about 5MB/s rate of video stream for usual cameras)

From Complex Event processing (CEP : RulesDefiner; THALES Artificial intelligence application should be able, to perform correlation rules definition when dealing with CEP (computing/building behaviour probabilities in order to recognize individual or atomic behaviour) in order to predict object/people behaviour

From IaaS Service Management; This module should enable allocation and configuration of virtual resources for large video data processing in short periods

From Publish/subscribe broker: This module should enable to send and listen raw event and correlated event provided by the CEP

The required functionality are:

- Video Tracking of people, cars
- Artificial Intelligence Engine
- Video Display
- 3D map display
- Video Recorder
- Clock synchronization
- Sensor discovery
- Sensor localization
- Video data encryption

The following features are expected from these enablers.

The following additional enablers maybe used (more information are necessary about the enablers) :

- Iaas Service Management
- Pre-processing of meta data
- IoT resources management
- PrimeLfie policy language
- Identity and privacy management
- Security monitoring
- SLA management

13.2.3 Environmental sensor Enablers

The following enablers are needed: IoT Communication, Secure Data Communication

From IoT Communication: Front-end; This module should implement methods for clock synchronisation

From Secure Data Communication: It should be possible to have communication security implemented in different network layers.

The required functionality are:

- Gateway discovery
- Clock synchronization
- Localization
- Pre-fault detection
- Secure and trusted communication and identification
- Capability announcement
- In-sensor data storage
- In-sensor data processing
- QoS and prioritizing
- Energy-efficiency.

The following features are expected from these enablers.

The following additional enablers maybe used (more information are necessary about the enablers) :

- Meta-data Pre-processing
- IoT Process Automation
- Identity management
- Multimedia analysis
- Connected Devices Interfacing
- Cloud Edge
- Network Information and Control
- Service, Capability, Connectivity and Control (S3C)

13.2.4 Gateway Enablers

The following enablers are needed: Complex Event Processing (To Be Used), Big Data Processing, Cloud Edge/Cloud Proxy (To Be Used), Semantic Annotation, Semantic Application Support, Metadata Pre-processing (To Be Used), Network Information & Control (NetIC) (To Be Used).

From Semantic Annotation: SemanticsFusion; To take the ontology priorities defined in STORY.SafeCity.Data.SemanticAnnotation/SemanticApplicationSupport.OntologyPriorities and use them as rules and criteria for shaping logic outcomes and classifications The following features are expected from these enablers.

From Semantic Annotation Support: OntologyPriorities; To determine the most frequent applications of data being preferred by the user, so as to deduce priorities for the delivery of her final output.

The required functionality are:

- Automatic Handling and classification of complex and vast amounts of data to be processed in real time (low latency)
- Temporary hosting of vast amounts of amount prior to being sent to the network
- Custom ontology definitions according to processing techniques
- Data search and categorization upon semantics
- QoS and network traffic management
- Hosting processing algorithms to locally examine the data
- Semantic Annotations of data (enriched content)
- Automatic definition of user priorities based on most common ontology uses
- Data fusion upon semantics definitions and priorities (as defined above)

The following features are expected from these enablers.

The following additional enablers maybe used (more information are necessary about the enablers) :

- IaaS Data Center Resource Management
- IaaS Cloud Edge Resource Management
- Localization Platform
- Multimedia analysis
- IoT Data Handling
- Connected Devices Interfacing
- Security Monitoring
- Identity Mixer
- IaaS Service Management
- PaaS Service Management
- SLA Management
- Resource Monitoring
- IoT Resources management
- Gateway Enablers – Mediation
- Identity Management.

13.2.5 Data Fusion Enablers

The following enablers are needed: Semantic Application Support GE.

From Semantic Application Support GE: StorageLayer; It is advisable for the Semantic Application Support to provide a storage layer providing storage for semantic based metadata. Therefore, the repository would storage RDF triples, while the registry would storage Ontologies making them available in order to consult or modify. Both repository and registry should meet strong security, scalability and performance requisites in order to support large scale applications. As a consequence, the knowledge can be accessed, modified or and queried in a scalable and secure way.

Reasoner engine; It is advisable for the Semantic Application Support to provide a Reasoner Engine, providing an automatic way to infer knowledge. As a consequence, the Reasoning component will make possible the generation of new knowledge from current knowledge and ontologies.

OntologyManager; It is advisable for the Semantic Application Support to provide an Ontology manager, allowing ontology browse and ontology edition. As a consequence, the Ontology manager, will make possible for the users to navigate and visualize through ontology network, also will allow edit the ontology stored in the system.

SearchEngine; It is advisable for the Semantic Application Support to provide an Search Engine, allowing to perform queries in semantic way. As a consequence, the Search Engine, will make possible for the users to performs queries, showing not only the matches elements, but also the relationships between them.

ParallelReasonerEngine; As a Data Management user, I would like to have an Enabler that allow me process huge amounts of previously stored data in order to obtain relevant insights in scenarios where latency can be a key factor or not (for the reasoning engine not is a key factor). This enabler will allow infer new knowledge from previously stored one in a transparent and parallel way.

The required functionality are:

- Ontology Management
- Database Storage (terns)
- Reasoning Engine
- Manual Annotation
- Search Engine
- API and Visualization Interface

The following features are expected from these enablers.

The following additional enablers maybe used (more information are necessary about the enablers) :

- Big Data Processing
- Complex Event Processing
- Multimedia analysis to gather multimedia meta-data
- Pre-processing of meta-data during/after gathering
- IoT Communications
- Security Monitoring
- Identity Management
- Localisation Platform
- Publish/Subscribe Broker

13.2.6 Decision Support Enablers

The following enablers are needed: Semantic Complex Event Processing, Publish/Subscriber Broker, Big Data Processing.

The required functionality are:

- Database Storage
- QoS and prioritization
- Clock synchronization
- Identity management
- Authentication, verification, privacy
- Service Level Agreement

- Big Data Processing

The following features are expected from these enablers.

The following additional enablers maybe used (more information are necessary about the enablers) :

- Complex Event Processing (CEP)
- Big Data Processing
- Publish/Subscriber broker
- Pre-processing of meta-data during/after processing
- Monitoring
- Identity management
- SLA Management
- Pre-processing of unstructured data during/after gathering
- Resource Metering and Accounting
- Security monitoring

13.2.7 Information Security Enablers

The following enablers are needed: IoT Communications GE (Including IoT Communications.Front-End e IoT Communications.Connectivity Management), IoT Resources Management GE (Including some specifical Enablers as IoTResourceManagement.Services&Resources Interaction), Security Monitoring GE, Security Manager, Settings Configuration, Localisation Platform, Data Handling, Trust Management

From IoT Communications (Including some specifical Enablers as IoT Communications.Front-End e IoT Communications.Connectivity Management);

IoT Communications.Front-End: It should be possible for the IoT Services Enablement platform to support the co-existence of a variety of existing and emerging communication technologies in order to allow the connection to the Internet of Things environment of a broad range of different hardware devices. The heterogeneous nature of sensor networks, RFIDs and embedded systems requires a flexible and interopeble solution to enable seamless interaction between high-level services and underlying deployed networks. As a consequence, the Front-End GE must specify a communication abstraction layer in order to integrate different underlying protocols used by all incorporated devices/gateways.

IoT Communications.Connectivity Management: It should be possible for the IoT Services Enablement platform to support possible mobility of different parts of any deployed network when (i) a mobile host dynamically changes its point of attachment to a fixed backbone, (ii) a network in motion dynamically changes its point of attachment to a fixed backbone, and, (iii) the backbone topology itself consists of mobile routers (leading to frequent topology changes). The requirement on mobility affects the Communication Protocol Adapter since it must be enhanced with technologies for supporting non-static network deployments. As a consequence, intelligent configuration and maintenance of any routing and/or naming network mechanism is mediated through a flexible Connectivity Management system.

From IoT Resources Management GE (Including some specifical Enablers as IoTResourceManagement.Services&Resources Interaction); It should be possible, for the IoT applications and end users, to discover, utilise, and activate small or large groups of IoT resources and manage their properties under the presence of hetergeneous identification and addressing schemes

that will be used to access the devices. For the Internet of Things, it is beneficial to find information and services associated to both things and IoT resources (and implicitly the device hosting them), and their mapping into network resources. As a consequence, the Services&Resources GE must specify/implement an abstract resource modelling for successful resource lookup and discovery, as well as, a fully remote management system enabling the initial configuration, activation, software update, de-activation, and re-activation of all IoT resources.

From Security Monitoring: Security Monitoring system for detecting potential attacks and/or non-authorized usage; It should be possible to continuously collect and monitor raw data (from large-scale heterogeneous environments) in order to achieve the execution of services with desired security behaviour and detection of potential attacks or non-authorized usage. In such a way appropriate actions, towards preventing and mitigating the impact of cyber-attacks, can be taken against constantly evolving threats. As a consequence, intelligent early attack detection and support for decision and rapid action making are mediated through a flexible Security Monitoring system.

From Security Monitoring: Implementation of an intelligent Intrusion Detection System capable of supporting the automated selection of countermeasures for the Security Monitoring platform; It is advisable for the Security Monitoring platform to provide an automated mechanism for detecting any ongoing intrusion attempt that can lead to an unauthorized access or alteration of the system's functionality. Appropriate mitigation responses, based on specific attack patterns and events involved in the attack, must be taken when necessary. As a consequence, an intelligent Intrusion Detection System for detecting any abnormal network behaviour must be implemented.

From Security Manager; It should be possible to support the secure exchange of all network traffic regardless of sensor hardware and communication protocol heterogeneity, value range, precision or unit. In such a way, through a transparent process (to the hosting IoT device/gateway), all outgoing traffic is encrypted (before transmission) and decrypted upon reception and before processing. As a consequence, adaptability in the applied security services is mediated through an intelligent Security Manager enabler for mapping them with the security needs of each communication.

From Setting Configuration; It is advisable for the Security Manager system to support the creation and configuration of various security profiles based on context information provided by middleware services such as service discovery, node discovery, location positioning, etc. In such a way, we can cope with different situations by maintaining different policy sets according to the security and privacy needs, the device capabilities, the service and the user preferences. As a consequence, policies that can enable or disable some of the security components or adjust their configuration (e.g., enhance or relax the parameters for secure communications) must be handled by the Settings Configuration enabler.

From Localisation Platform; It should be possible to know when and where an event was triggered and/or measured in order to develop secure context-aware IoT applications. In such a way, an efficient trust relationship scheme can be produced for deployed devices in various network regions. In scenarios where the IoT SE platform supports the mobility of any underlying heterogeneous devices, it is beneficial to be able to retrieve mobile device positions and localization area events. As a consequence, the Localisation Platform GE must address issues related to localization of mobile devices even when the use of GPS equipment is not feasible (e.g., urban canyons where the GPS receiver cannot acquire sufficient GPS signals).

From Data Handling; It should be possible to secure the exchange of information between networking IoT devices and gateways in order to ensure the security and integrity of transmitted data. In such a way, we address concerns related to confidentiality, security, and preservation/retention of produced data. As a consequence, automated resources pertaining to confidential data processing (e.g., encryption, decryption) and transmission through authenticated message exchange must be mediated through the secure Data Handling enabler.

From Trust Management; It should be possible to specify, evaluate, establish, and ensure the trust relationships among IoT devices/gateways. In particular, values must be adaptively adjusted based on run-time trust assessment in order to reflect real system context and situation. Such functionalities are required for nodes that will need to communicate with nodes different from those that they were initially configured to trust. As a consequence, the trust level of a node's produced data/events must be measured/evaluated by the Trust Management enabler.

The required functionality are:

- Connectivity Manager
- Heterogeneity of Sensors
- Security Manager
- Trust management
- Security protocol and mechanism
- Node/Service Discovery
- Localization support
- Security Monitoring
- Intrusion Detection & Communication Security

The following features are expected from these enablers.

The following additional enablers maybe used (more information are necessary about the enablers) :

- Generic Enablers for Gateway
- Mobility Analysis
- Context-based security and compliance
- Identity and Privacy management
- Security protocol and mechanism
- IoT Data Handling & Naming
- Network Information and Control
- PrimeLife Policy Language (PPL) Engine

13.2.8 Ad Hoc Networks Enablers

The following enablers are needed: Network Information and Control, IoT Communications, IoT Data Handling, Cloud Edge, Data/Context Management.

From Network Information and Control (NetIC): Ad hoc networks; Ad hoc networks for replace damage network communication infrastructures,

Nodes self-configuration; Ad hoc nodes can self-configuring after turned on,

Ad hoc Routing Protocol; Packet routing between ad hoc network nodes,

From IoT Communications : Ad hoc network nodes traffic; Deals with incoming/outgoing traffic from/to ad hoc network nodes

Ad hoc network nodes content control; Manage traffic flow, access policy control and quality of service.

From Cloud Edge: Ad hoc Network; Exchange data between ad hoc network and FI-WARE cloud gateway,

The required functionality are:

- Nodes self-configuration
- Nodes Monitoring
- Nodes Authentication
- Group Communication
- Routing
- Support voice, data, image and video transportation
- Data Encryption
- Nodes Localisation

The following features are expected from these enablers.

The following additional enablers maybe used (more information are necessary about the enablers) :

- Real-time recommendations
- IoT Process Automation
- Service, Capability, Connectivity and Control (S3C)
- IoT Data handling
- Connected Devices Interfacing

14. Annex : feature backlog entries

BacklogEntries_SYNTHESIS_V1.xls

Cf. table in the document “BacklogEntries_SYNTHESIS_V1.xls”.

Stakeholder	Id	Name	Goal	Scope	Chapter	Enabler	Description	Rationale
ARA	SAFECITY.STORY.DATA/CONTEXT MANAGEMENT.SemanticApplicationSupport.SemanticsFusion	SemanticsFusion	To take the ontology priorities defined in STORY.SafeCity.Data.SemanticAnnotation/SemanticApplicationSupport.OntologyPriorities and use them as rules and criteria for shaping logic outcomes and classifications	Application	Data/Context Management	Semantic Annotation, Semantic Application Support	The feature is going to import data from the STORY.SafeCity.Data.SemanticAnnotation/SemanticApplicationSupport.OntologyPriorities and consider the proposed priority levels as guidelines of categorization. Search in the semantics patterns will allow identification of the ontologies describing each data package being delivered. In this way, clusters of data are going to be formed, corresponding to each major priority, and representing a set of user and application oriented information packages presenting common descriptions.	The feature can be used to gather and combine large and/or complex data, by following user and application criteria for definying their rationales. Accordingly, the feature's output can be used to further develop in a similar way QoS delivery to the user.
ARA	SAFECITY.STORY.DATA/CONTEXT MANAGEMENT/SemanticApplicationSupport.OntologyPriorities	OntologyPriorities	To determine the most frequent applications of data being preferred by the user, so as to deduce priorities for the delivery of her final output	Application	Data/Context Management	Semantic Annotation, Semantic Application Support	The feature will keep an updated record of changes in ontology engineering realized across the applications being used by the user and will acquire based on logs and search by pattern results, information on the most commonly used semantics. The frequency of each semantic annotation will be translated into variable levels of user preferences and thus priorities.	The feature proposed will keep track of the most commonly used semantic keywords used by applications, processing the user data. These frequencies would imply the application focus of the user and in turn his criteria for evaluating and reviewing information. The feature will then update a list of most common patterns, also be seen as priorities, which can then be accessed by other features and enablers, e.g. QoS, data fusion, etc
THA	SAFECITY.STORY.DATA/CONTEXT MANAGEMENT.Data.broker.switchCEP	switchCEP	This module should enable to send and listen raw event and correlated event provided by the CEP	Platform	Data/Context Management	Publish/subscribe broker	This module should allow to publish and subscribe to every event, raw event (inputs of the CEP application) and corralated event (outputs of the CEP application)	Enable communication between CEP enabler, raw events and THA Artificial Intelligence application
THA	SAFECITY.STORY.DATA/CONTEXT MANAGEMENT.Data.BigDataProcessing.BigVideo	BigVideo	This module should allow the use of large bandwith and large storage for video analysis purposes (about 5MB/s rate of video stream for usual cameras)	Platform	Data/Context Management	Big Data Processing	This module should allow to access simultaneously to a large set of video streams, either coming from sensors or from storage areas, with a high QoS	Video Analysis SaaS. It will be one of the future uses of video analysis.
THA	SAFECITY.STORY.DATA/CONTEXT MANAGEMENT.Data.CEP.RulesDefiner	RulesDefiner	THA Artificial intelligence application should be able, to perform correlation rules definition when dealing with CEP (computing/building behaviour probabilities in order to recognize individual or atomic bahaviour) in order to predict object/people behaviour	Platform	Data/Context Management	CEP	Define listen (operationally relevant) events, define correlation (between real time - < 100 ms latency - events) rules, alert in real time when a correlation rule happend.	Identify people/object behaviour pattern in order to forecast coming actions
THA	SAFECITY.STORY.CloudHosting.VideoIaaSServiceManagement	VideoIaaSServiceManagement	This module should enable allocation and configuration of virtual resources for large video data processing in short periods	Platform	Cloud hosting	IaaS Service Management	Provide defined amount of CPU and memory for deploying Video SaaS. Video analysis needs are mostly constant through time once the application and number of video streams are chosen.	Need for large processing resources for video analysis
THA	SAFECITY.STORY.DATA/CONTEXT MANAGEMENT.MultimediaAnalysis.SpecificMetaDataHandling	SpecificMetaDataHandling	This module should enable to annotate inputs and outputs of proprietary and business specific video analysis module. //The API provided must enable to embed a "multimedia stream analysis" 3rd party (indeed, this function is business specific).	Platform	Data/Context Management	Multimedia Analysis	This module should allow to annotate and store inputs and outputs of the video processing steps. Inputs metadata should contain video format, timestamp, sensor localisation information, and also context-based annotation such as luminosity condition. The output metadata should contain video processing results from object to event .	video analysis metadata annotation

HIB	SAFECITY.Story.DATA/CONTEXT MANAGEMENT.Data.SemmanticApplicationSupport.StorageLayer	StorageLayer	It is advisable for the Semantic Application Support to provide a storage layer providing storage for semantic based metadata. Therefore, the repository would storage RDF triples, while the registry would storage Ontologies making them available in order to consult or modify. Both repository and registry should meet strong security, scalability and performance requisites in order to support large scale applications. As a consequence, the knowledge can be accessed, modified or and queried in a scalable and secure way.	Application	Data/Context Management	Semantic Application Support	This User Story provides a storage layer providing storage for semantic based metadata in a scalable and secure way.	To achieve the goal is mandatory store terns using a semantic database.
HIB	SAFECITY.Story.DATA/CONTEXT MANAGEMENT.Data.SemmanticApplicationSupport.ReasonerEngine	Reasoner engine	It is advisable for the Semantic Application Support to provide a Reasoner Engine, providing an automatic way to infer knowledge. As a consequence, the Reasoning component, will make possible the generation of new knowledge from current knowledge and ontologies.	Application	Data/Context Management	Semantic Application Support	This module generates new knowledge from previous knowledge stored ones.	In order to infer new knowledge is mandatory to use some Reasoner Engine.
HIB	SAFECITY.Story.DATA/CONTEXT MANAGEMENT.Data.SemmanticApplicationSupport.OntologyManager	OntologyManager	It is advisable for the Semantic Application Support to provide an Ontology manager, allowing ontology browse and ontology edition. As a consequence, the Ontology manager, will make possible for the users to navigate and visualize through ontology network, also will allow edit the ontology stored in the system.	Application	Data/Context Management	Semantic Application Support	This module allows to define an Ontology, in manner that all knowledge can be classified according this Ontology. Moreover this module must allow to modify the Ontology.	The knowledge and the SafeCity's semantics should be defined according to an Ontology.
HIB	SAFECITY.Story.DATA/CONTEXT MANAGEMENT.Data.SemmanticApplicationSupport.SearchEngine	SearchEngine	It is advisable for the Semantic Application Support to provide an Search Engine, allowing to perform queries in semantic way. As a consequence, the Search Engine, will make possible for the users to performs queries, showing not only the matches elements, but also the relationships between them.	Application	Data/Context Management	Semantic Application Support	This module allows performing queries, showing matches elements and relationships between them.	The module must provide a feature in order to allow user make searches.
HIB	SAFECITY.EPIC.DATA/CONTEXT MANAGEMENT.Data.BigDataAnalysis.ParallelReasonerEngine	ParallelReasonerEngine	As a Data Management user, I would like to have an Enabler that allow me process huge amounts of previously stored data in order to obtain relevant insights in scenarios where latency can be a key factor or not (for the reasoning engine not is a key factor). This enabler will allow infer new knowledge from previously stored one in a transparent and parallel way.	Application	Data/Context Management	Semantic Application Support	The Big Data Analysis GE will allow developer to process big data set using a transparent and really simple API for parallelization and distribution.	The number of new events in SafeCity grows at rate of 432GB per day[1], it's desirable this enabler in order to process huge amount of data and infer new knowledge.
TEK	SAFECITY.EPIC.I2ND.NetIC.GE	Ad hoc networks	Ad hoc networks for replace damage network communication infrastructures	Platform	I2N	NetIC	Ad hoc networks are formed by several communication nodes that are deployed on the incident/intervention area and are able to self-configuring after turned on. These communication nodes can transmit data from sensors, voice from safety crew, messaging data, images and video.	It should be possible to replace the network communication infrastructures after incidents that damage or disable them. Ad hoc networks provide a quick deployment of the network with minimal configuration. Ad hoc networks can provide communication on the incident area as also establish a link to the Internet or other network. Command centre can receive information about statistics and network utilization.
TEK	SAFECITY.STORY.I2ND.NetIC.GE.SelfConfig	Nodes self-configuration	Ad hoc nodes can self-configuring after turned on	Platform	I2N	NetIC	Nodes can find a proper network address and start negotiating with neighbor nodes	For a quick deploy, nodes should perform by it self configuration tasks automatically.
TEK	SAFECITY.STORY.I2ND.NetIC.GE.Routing	Ad hoc Routing Protocol	Packet routing between ad hoc network nodes	Platform	I2N	NetIC	Routing protocol should be based on energy, location and link quality.	Typically, ad hoc nodes communicate through wireless links and they rely on battery power supply. So, routing protocol should consider nodes energy level as also localisation, since RF transmission can consider the distance between nodes to save power.
TEK	SAFECITY.STORY.CE.GE.Gateway	Ad hoc Network Gateway	Exchange data between ad hoc network and FI-WARE cloud	Platform	I2N	CE	One or more devices can be connected to the Internet or private network to retransmit ad hoc network data to the command centres.	Data from ad hoc networks can be important to support decisions on the command centre. Also the command centre can send action orders to ad hoc network nodes for a better operation coordination.
TEK	SAFECITY.STORY.CDI.GE.PSApps	Public Safety Applications	Applications for public safety	Platform	I2N	CDI	Citizens and safety players applications to receive or report information about public safety.	Multiple channels can be consered to transmit the data: 3G, Wi-Fi, Ad hoc networks, etc.

TEK	SAFECITY.STORY.IoTCommunications.Front-end.GE	Ad hoc network nodes traffic	Deals with incoming/outgoing traffic from/to ad hoc network nodes	Platform	I2N	IoT Communications	Traffic exchange between ad hoc nodes. This enabler relies on security, privacy and trust GE for security issues (encryption).	
TEK	SAFECITY.STORY.IoTCommunications.ContentContro	Ad hoc network nodes content control	Manage traffic flow, access policy control and quality of service.	Platform	I2N	IoT Communications	Ad hoc networks monitoring. Support group communication between ad hoc nodes by configuring access control lists.	
TEK	SAFECITY.STORY.IoTDataHangling	Ad hoc network nodes data storage and logs	Store data and logs on each ad hoc network node.	Platform	I2N	IoTDataHangling	Each node should store data and logs regarding operation.	For example, one node for any reason can be disconnected from the ad hoc network temporarly and it still receive data from sensors that should be stored to be sent when the connection is restablished.
TEK	SAFECITY.STORY.Data.Localization.GE	Ad hoc network nodes location	Ad hoc networks provide nodes geo information to achieve a better coordination and management at command centre	Platform	I2N	Data/Context Management	Nodes can provide location based on thechniques such as A-GPS, WiFi or Cell-Id. At command centre can be visualized the location of all nodes.	Comman centre can get information from ad hoc network nodes to support decisions.
ATH-AIT	SAFECITY.Story.DATA/CONTEXT MANAGEMENT.Data.SemanticApplicationSupport.KnowledgeRepresentationDataModeling	KnowledgeRepresentationDataModeling	Definition of knowledge domain and multimedia ontologies, as well as metadata schemas within the context of the safety and security domains applied to video analytics	Apllication	Data/Context Management	Semantic Application Support	Safety and security-related knowledge models (domain and multimedia ontologies), taxonomies and respective data models will be introduced (up to Phase 2), for data interoperability among the SafeCity applications and in order to facilitate automated reasoning and inferencing on top of detected primitive events, objects, etc. during video analysis towards efficiently identifying emergency events or suspicious behaviours. These knowledge and data models will allow for spatial and/or time-based co-occurrences of detected spatio-temporal patterns (e.g. movement), objects or event primitives in video data that are in line with the “rules” dictated in the defined ontologies.	The ontology and metadata editor tools should be available to easily define such as per application need.
ATH-AIT	SAFECITY.Story.DATA/CONTEXT MANAGEMENT.Data.SemanticApplicationSupport.DataMetadataHandling	DataMetadataHandling	Management of video data (archived and streams) as well as metadata instances	Platform	Data/Context Management	Semantic Application Support	Appropriate editor as well as parsing tools are necessary for creating/updating the above mentioned knowledge models and metadata schemas, such as Protégé for ontologies or the Xerces XML parser for XML-based metadata, as well as for encoding/decoding, playing back and streaming video data.	
ATH-AIT	SAFECITY.Story.DATA/CONTEXT MANAGEMENT.Data.SemanticApplicationSupport/ObjectStorage.DataMetadataStorage	DataMetadataStorage	Storing and retrieving video data and metadata instances as well as other mandatory data (data models, ontologies) into archive system	Platform	Data/Context Management	Semantic Application Support, Object Storage (?)	Furthermore, with respect to their storage, video data and metadata are expected to be stored in the generic Safecity C2 respective archive while Data models, Ontologies, Rules, etc. compose the generic Safecity Knowledge repository	
ATH-AIT	SAFECITY.Story.DATA/CONTEXT MANAGEMENT.Data.SemanticApplicationSupport.ReasoningEngine	ReasoningEngine	To reason out based on visually detected patterns, events, etc. and their spatio-temporal co-occurences, based on Safecity ontology and respective rules, higher level semantics as concerns suspicious behaviour detection	Platform	Data/Context Management	Semantic Application Support	Includes inference algorithms based on e.g. description logics or FOL and operates on top of the defined Safecity Ontologies and associated rules in order to infer higher level semantics with respect to situation insights. Reasoning is focused mainly on how to assess the spatiotemporal sequence of a variety of detected objects and event primitives in the video stream into a semantically defined suspicious behaviour instance, existent in the Safecity safety ontology.	

ATH-AIT	SAFECITY.Story.DATA/CONTEXT MANAGEMENT.Data.SemanticApplicationSupport.MetadataGenerationParsing	MetadataGenerationParsing	To provide functionalities for instantiating metadata descriptions based on detection results to be communicated to other Video analytics components or other Safecity applications, as well as to provide the tools to parse effectively such instances based on the defined (stored) metadata schemas	Platform	Data/Context Management	Meta-data pre-processing; Semantic Annotation GE	Component that allows the automatic generation of metadata instances following the adopted metadata schemas, carrying semantic, structural, operational and low-level information on visually processed data and the situation insights produced. It is further required that the ability to search among metadata and parse them is provided e. g. for the case of retrieving past data from the Safecity data archive, or in case that other Safecity applications are parsing the metadata information such as the Data Fusion or Decision Support System applications (data interoperability of data exchanges among diverse SafeCity applications).	
ATH-AIT	SAFECITY.Story.DATA/CONTEXT MANAGEMENT.Data.SemanticApplicationSupport.OntologyEvolution	OntologyEvolution	To provide the ability to evolve the captured know-how (in the Safecity ontology) based either on new suspicious behaviours observation, user inputs, or detection results (from other applications as well, coming from Data Fusion and DSS systems)	Platform	Data/Context Management	Semantic Application Support	Updates ontological definitions and associated inference rules based on new findings (assisted also by the Data Fusion and DSS systems) as well as C2 personnel observations (through interactions) in dynamic video data with respect e.g. to new behavioral patterns or limited efficiency of the initial ontology to capture a specific event instance.	The detection system is thus kept updated to latest observations with respect to evolution of suspicious behaviours
ATH-AIT	SAFECITY.Story.DATA/CONTEXT MANAGEMENT.Data.MultimediaAnalysis.VideoProcessing&AnalysisEngine	VideoProcessing&AnalysisEngine	To provide the required video processing and analysis algortihms in order to visually perceive potential threat cases in camera monitored areas	Platform	Data/Context Management	Multimedia Analysis	Component that includes a rich set of automated or semi-automated (where required) image/video processing algorithms such as: Region/Object segmentation (car, person, animal, vehicle, etc.) by color, shape, texture, edges, etc. Motion Estimation Moving Object Segmentation Moving Object Tracking (person, vehicle, animal, etc.) Foreground/Background Detection Face detection Face identification Orphan object detection Car detection and tracking Licence Plate recognition Line drawing Change detection Activity Detection Event Classification and Detection (use of the respective ontology and pattern recognition algorithms) Suspicious Behaviour Classification and Detection (use of the respective ontology and pattern recognition algorithms) such as detection of loitering, fights, races, falls, movement against the flow of traffic, etc. A sub-component of the engine further performs video pre-processing for video content filtering and selective video	The efficiency of the video analytics engine and its real-time operation are crucial factors in automated camera-enabled surveillance systems
ATH-AIT	SAFECITY.Story.DATA/CONTEXT MANAGEMENT.Data.MultimediaAnalysis.VisualDescriptorsExtraction	VisualDescriptorsExtraction	To provide the capability to process and extract meaningful visual descriptors that uniquely characterize specific objects, events, patterns in video data.	Platform	Data/Context Management	Multimedia Analysis	The component aims to extract, through video analysis and feature extraction algorithms, visual descriptors from previously segmented spatial, temporal or spatio-temporal regions. The purpose is to efficiently describe visual primitives from video data with low-level visual metadata that will further serve as input to either the pattern recognition modeling phase (during training assuming that the required amount of training video data is available) or the detection/matching phase.	

ATH-AIT	SAFECITY.Story.DATA/CONTEXT MANAGEMENT.Data.MultimediaAnalysis.PatternRecognition	PatternRecognition	To allow during the training/learning phase the generation of optimal visual data models (face identities, object models, movement pattern models, etc.), that will assist and speed up the detection phase	Platform	Data/Context Management	Multimedia Analysis?	Both classification (SVM, LVQ, etc.) and clustering (density-based, etc.) algorithms will formulate a pattern recognition engine that will be used, having as input visual feature vectors (single or combined), to either produce object, behaviour or primitive event models during the training phase of supervised learning algorithms using training video data from prior threatening events, or generate clusters of such entities using video data from prior threatening events for which respective apriori knowledge does not exist, or detect and identify during the testing phase of both classification or clustering algorithms the situation hint (object, primitive event or behaviour) during the overall process of situation insights generation. The modelling phase generates behavioural models and detected patterns in visual data from previous similar public safety threat events in archived video feeds, while the detection phase is assisted by them to identify the exact detected object or primitive event/behaviour in the currently monitored video feed.	
ATH-AIT	SAFECITY.Story.DATA/CONTEXT MANAGEMENT.Data.MultimediaAnalysis.ModelRetraining	ModelRetraining	To enhance the detection efficiency of the video analytics application	Platform	Data/Context Management	Multimedia Analysis?	It is often the case that learned models in classification algorithms or clusters in clustering algorithms, due to insufficiency of training data or noisy data, are often not optimal or fail to represent the full potential of a specific concept or entity. With the provision of new video data through the constant monitoring process, these serve as input for model retraining (running the classification and clustering algorithms to reproduce models or clusters) in case that this process leads to higher accuracy of the latter. Furthermore, the validation of detection results by human operators at the Command Centre facilitates this process even more and with a higher accuracy. Both these tasks are considered in a component dealing with model retraining	
VTT	SAFECITY.STORY.Security.SecureDataCommunication	Secure data communicatio over network	It should be possible to have communication security implemented in different network layers.	Platform Generic	Security	Secure Data Communication	This module should provide secure data communication over heterogeneous networks. Today secure data communication can be provided in link, network and transport layers with e.g. MACsec, IPsec, and SSL/TSL protocols.	To achieve secure data communication is mandatory. It is also needed in order to meet ethical and legal requirements.
VTT	SAFECITY.STORY.IoT.IoTCommunications.FrontEnd	Front-end	This module should implement methods for clock synchronisation.	Platform Generic	IoT	IoT Communications	This module should provide method for clock synchronisation of IoT devices. On Ethernet based networks one such protocol could be IEEE-1588 as one of its design criteria is to be lightweight and accurate.	Accurate time in sensors is crucial for time dependent events or for timely coordinated control of sensors and actuators.
AIT	SAFECITY.Theme.Security.Security Monitoring GE.Intrusion Monitoring & Response	Intrusion Monitoring & Response	It should be possible to continuously collect and monitor raw data (from large-scale heterogeneous environments) in order to achieve the execution of services with desired security behavior and detection of potential attacks or non-authorized usage. In such a way appropriate actions, towards preventing and mitigating the impact of cyber attacks, can be taken against constantly evolving threats. As a consequence, intelligent early attack detection and support for decision and rapid action making are mediated through a flexible Security Monitoring system.	Platform	Security	Security Monitoring	Security monitoring is focused essentially on monitoring alarms from network equipment, systems and security sensors. By the collection, filtering and correlation of data, including sensitive data from security tools and devices, raw sensor data, suspicions behaviours, etc., coupled with a dynamic risk analysis engine, decision making support and role-oriented visualization engine, the security stakeholders can take appropriate actions to prevent and mitigate the impact of abnormal behavior.	Any part of the already deployed sensor networks can be a possible point of intrusion, since all nodes act as generators/routers of information and they can be manipulated or subverted by cyber attackers. Therefore, it is essential to have an intelligent security monitoring system that is able to prevent/detect common threats and new ones that have not been anticipated before in order to initiate proper responses.

AIT	SAFECITY.Story.Security.Security Monitoring GE.IntrusionDetection & Response Engine	Intrusion Detection	It is advisable for the Security Monitoring platform to provide an automated mechanism for detecting any ongoing intrusion attempt that can lead to an unauthorized access or alteration of the system's functionality. Appropriate mitigation responses, based on specific attack patterns and events involved in the attack, must be taken when necessary. As a consequence, an intelligent Intrusion Detection System for detecting any abnormal network behaviour must be implemented.	Platform	Security	Security Monitoring	Intrusion detection is a monitoring methodology for defining a suitable intrusion model, based on which is possible to distinguish between normal and abnormal activities in order to discover malicious attempts in time. Main techniques for identifying attack behaviour patterns/paths are: misuse, anomaly and specification-based detection. Based on the results of this ID functionality, appropriate mitigating actions and countermeasures must be selected in an automated (or semi-automated) manner. These can involve changes in the established network status, update of any cryptographic material, reformation of affected node trust relationships, etc.	Network services will always be exposed to different types of threats that can lead to severe misuse and damage. Inherent vulnerable characteristics make them susceptible to a wide range of attacks that once applied, it may be too late before any counter action can take effect. It is therefore beneficial to constantly (or at least periodically) monitor all network operations in order to identify any suspicious behavior and take appropriate countermeasures. Such a mechanism will guarantee the execution of services with desired security behaviour.
AIT	SAFECITY.Theme.Security.Context-based Security & Compliance GE.CB Security Level Scheme	Context-based Security Level Scheme	It should be possible to fulfil various security requirements requested by different sets of applications in order to achieve the best security behavior for deployed devices and resources. Associated *security levels* will enhance the confidentiality and integrity of sensitive data context especially in crisis management scenarios. As a consequence, classification of various security levels/enablers based on communicated data context is mediated through a flexible Context-based Security scheme.	Platform	Security	Context-based Security & Compliance	The Context-based Security & Compliance GE supports additional security requirements requested by various sets of applications as a result of the applications's information context and specific regulatory constraints. It accepts security requests from a client application and selects the best security enabler/level to fulfil it. The deployed security enabler will implement the compliance between the client security request and any defined regulation. The framework has also monitoring capabilities to overseen the system performance.	IoT application environments allow the communication of various types of network traffic. The data context of this traffic defines the *significance* and *importance* of the transmitted information. For some information, like in crisis management scenarios, it is essential not to have any kind of leakage to any unauthorized entity. It is therefore beneficial to associate security levels (e.g., low, medium, high) with data context for ensuring (according to application requirements) the confidentiality and integrity of all network communications.
AIT	SAFECITY.Epic.IoT.IoT Communications Front-End GE.Network Communication	Network Communication	It should be possible for the IoT Services Enablement platform to support the co-existence of a variety of existing and emerging communication technologies in order to allow the connection to the Internet of Things environment of a broad range of different hardware devices. The heterogeneous nature of sensor networks, RFIDs and embedded systems requires a flexible and interoperable solution to enable seamless interaction between high-level services and underlying deployed networks. As a consequence, the Front-End GE must specify a communication abstraction layer in order to integrate different underlying protocols used by all incorporated devices/gateways.	Platform	IoT	IoT Communications.Front-End	The Front-end GE deals with the incoming/outgoing traffic from/to Devices and IoT Gateways. It comprises a number of Connection Protocol Adapters and a component dealing with the Communication Protocol Abstraction Definition. Each of the Connection Protocol Adapters is capable of handling one of the protocols that are accepted in FI-WARE, translating it into a unique internal language, which normalizes the different communication protocols within the platform.	IoT application environments are extremely heterogeneous pronouncing variety of underlying used communication layers. Therefore, it is essential for the IoT SE platform to support the connection, interaction and generic access to any kind of deployed embedded device regardless of the hardware type. This makes unavoidable the development of a front-end layer.
AIT	SAFECITY.Epic.IoT.IoT Communications Connectivity Management GE.Connectivity Interfaces	Connectivity Interfaces	It should be possible for the IoT Services Enablement platform to support possible mobility of different parts of any deployed network when (i) a mobile host dynamically changes its point of attachement to a fixed backbone, (ii) a network in motion dynamically changes its point of attachement to a fixed backbone, and, (iii) the backbone topology itself consists of mobile routers (leading to frequent topology changes). The requirement on mobility affects the Communication Protocol Adapter since it must be enhanced with technologies for supporting non-static network deployments. As a consequence, intelligent configuration and maintenace of any routing and/or naming network mechanism is mediated through a flexible Connectivity Management system.	Platform	IoT	IoT Communications.Connectivity Management	The Connectivity Management GE deals with lower level layers of the communication from/to Devices, IoT Gateways and the Content Control block with higher level layers. It consists of components dealing with Session Management, Mobility Management and Discontinuous Connectivity Management. The Mobility Management deals with the Devices and IoT Gateways mobility, both the connection through different Access Networks and the physical mobility of the "things". The Discontinuous Connectivity Management allows communicating between IoT Gateways and Devices that are not always on.	The diversity in network protocols (e.g., communication, routing, etc.) that can be used in static and non-static deployments for various contexts makes it mandatory for the IoT SE platform to be able to handle both types, if a variety of devices and gateways must be supported. It is thus a good architectural design to incorporate a flexible Connectivity Management system that is also able to operate in resource-constrained environments such as sensor networks where communicating parties might not always be on.

AIT	SAFECITY.Epic.IoT.IoT Resources Management.Services & Resources Interaction GE.Resource Configuration & Discovery	Resource Configuration & Discovery	It should be possible, for the IoT applications and end users, to discover, utilise, and activate small or large groups of IoT resources and manage their properties under the presence of heteregoneous identification and addressing schemes that will be used to access the devices. For the Internet of Things, it is beneficial to find information and services associated to both things and IoT resources (and implicitly the device hosting them), and their mapping into network resources. As a consequence, the Services&Resources GE must specify/implement an abstract resource modelling for successful resource lookup and discovery, as well as, a fully remote management system enabling the initial configuration, activation, software update, de-activation, and re-activation of all IoT resources.	Platform	IoT	IoT Resources Management. Services & Resources Interaction	The Services & Resources Interaction GE focuses on global identification and information model schemes, for IoT resources, providing a resolution infrastructure to link them with relevant things and developping a common management tool for configuring, operating and maintaining the IoT resources on a large scale and with minimum human intervention. This copes with the need of integrating various connectivity modules as well as software management: firmware updates, operating systems, and application logic.	It would make no sense to require from the IoT SE platform to support the operation of a single type of computational element (software running on the device). On the contrary, a correct architectural design requires minimal human intervention when managing the various deployed IoT resources. This requires the development of a common resource management tool that provides on-the-fly service discovery and program image distribution.
AIT	SAFECITY.Epic.IoT.IoT Communications Naming GE.Naming & Resolution Interface	Naming & Resolution Interface	It should be possible for the IoT Services Enablement platform to support the *identification* and *addressing* of heterogeneous IoT devices and gateways in order to be accessible by any running application and other incroporated components with the appropriate privileges. In such a way network traffic can be routed to/from any requested node. As a consequence, the Naming GE must implement a ubiquitous naming system providing sufficient interfaces for identifying devices regardles of their position and status (static or mobile).	Platform	IoT	IoT Communications.Naming	The Naming GE integrates heterogeneous identification, naming and addressing technologies for identifying all networking devices/gateways. Scalable discovery and look-up makes IoT devices and resources available to all types of applications considering important real-world aspects like location, time, availability, etc. It will also provide fully remote management of the devices, as well as, associations between IoT resources and things.	The immense scale of node deployment, that characterizes most of the IoT applications, makes it mandatory for the IoT SE platform to be able to identify each one of the networking devices. It is thus a good architectural design to incorporate a flexible and ubiquitous Naming system that is able to provide sufficient interfaces for addressing even the more distant network nodes.
AIT	SAFECITY.Theme.Data/Context.Localisation Platform GE.Event Localization	Event Localization	It should be possible to know when and where an event was trigerred and/or measured in order to develop secure context-aware IoT applications. In such a way, an efficient trust relationship scheme can be produced for deployed devices in various network regions. In scenarios where the IoT SE platform supports the mobility of any underlying heterogeneous devices, it is beneficial to be able to retrieve mobile device positions and localization area events. As a consequence, the Localisation Platform GE must address issues related to localization of mobile devices even when the use of GPS equipment is not feasible (e.g., urban canyons where the GPS receiver cannot acquire sufficient GPS signals).	Platform	Data/Context Management	Localisation Platform	The Localisation Platform GE aims to retrieve mobile device positions and localization area events. The localization GE is based on various positioning techniques such as A-GPS, WiFi and Cell-Id whilst taking into account the end-user privacy.	For many applications (especially in crisis management scenarios), it is important to know the position of a deployed mobile device that either changes its point of attachement to a fixed gateway or just enters the network (e.g., node addition). In such a way, the Security enabler can create and maintain an intelligent trust relationship scheme among the deployed devices for measuring/evaluating the quality of produced data events.
AIT	SAFECITY.Theme.CommSec.Security Manager SE	Security Manager	It should be possible to support the secure exchange of all network traffic regardles of sensor hardware and communication protocol heterogeneity, value range, precision or unit. In such a way, through a *transparent* process (to the hosting IoT device/gateway), all outgoing traffic is encrypted (before transmission) and decrypted upon reception and before processing. As a consequence, *adaptability* in the applied security services is mediated through an intelligent Security Manager enabler for mapping them with the security needs of each communication.	SAFECITY Communication Security Application	SAFECITY Communication Security Application	Security Manager	The Security Manager SE provides functionalities that include: • **Cryptographic protocols abstraction**: A mechanism to enable the support of different security policy sets (e.g., cipher suites, cryptographic protocols, etc) according to the application security needs. For instance, a “strong” security level parameter value will lead to the use of more sophisticated cryptographic techniques.	Any part of the already deployed sensor networks can be a possible point of intrusion, since all nodes act as generators/routers of information. Therefore, it is essential to have an intelligent security manager that is capable of securing all network communications and take measures that prevent threats like eavesdropping, integrity violations, masquerading and traffic analysis through the use or proper encryption and authentication methods.

AIT	SAFECITY.Epic.CommSec.Settings Configuration SE	Settings Configuration	It is advisable for the Security Manager system to support the creation and configuration of various security profiles based on context information provided by middleware services such as service discovery, node discovery, location positioning, etc. In such a way, we can cope with different situations by maintaining different policy sets according to the security and privacy needs, the device capabilities, the service and the user preferences. As a consequence, policies that can enable or disable some of the security components or adjust their configuration (e.g., enhance or relax the parameters for secure communications) must be handled by the Settings Configuration enabler.	SAFECITY Communication Security Application	SAFECITY Communication Security Application	Settings Configuration	The Settings Configuration SE addresses the configuration of all security primitives to be used by the overall Security Manager enabler. Provided *security levels* support the control of various cryptographic techniques and protocols (subject to the project's requirements). More specifically, the SC enabler may associate security levels/protocols with applications, groups of networking devices or even groups of established network channels. Once a security scheme has been associated to a thing, all of its security protocols are configured for later use to any underlying service. Security schemes include primitives such as appropriate keys to be used for encryption/decryption, cipher suites, cryptographic protocols, etc.	It would make no sense to require from the Security Manager to support *only* a specific subset of cryptographic protocols as this may not be required by all applications and, in the case of sophisticated security techniques, the power and computational resources may not be sufficient for their successful implementation. On the contrary, a correct conceptual design must be able to support different security policy sets according to the requested application needs and the context of the transmitted data. This requires the development of a flexible security settings configuration tool that creates profiles for all supported security enablers/levels and each time provides the best suited one.
AIT	SAFECITY.Epic.CommSec.Data Handling Se	Data Handling	It should be possible to secure exchange of information between networking IoT devices and gateways in order to ensure the *integrity* of transmitted data. In such a way, we address concerns related to confidentiality, security, and preservation/retention of produced data. As a consequence, automated resources pertaining to confidential data processing (e.g., encryption, decryption) and transmission through authenticated message exchange must be mediated through the secure Data Handling enabler.	SAFECITY Communication Security Application	SAFECITY Communication Security Application	Data Handling	The Data Handling SE provides the below components: •**Data Processing:** The data processing component is responsible for securing all network connections established by the FI-WARE IoT Communications GE. It deals with the low level encryption/decryption procedures performed on any data that is ready for transmission/reception. • **Message Stream Creation**: Component that creates the necessary packet stream to hold the encrypted data. It also deals with the attachment of any required MAC or digital signatures for ensuring message authentication and integrity.	Utilization of advanced encryption techniques is the best way for ensuring the *confidentiality* and *integrity* of transmitted data. It is thus beneficial to have a tool that incorporates such cryptographic protocols for handling successful transmission through a secure established communication channel.
AIT	SAFECITY.Epic.CommSec.Trust Management SE	Trust Management	It should be possible to specify, evaluate, establish, and ensure the trust relationships among IoT devices/gateways. In particular, values must be adaptively adjusted based on run-time trust assessment in order to reflect real system context and situation. Such functionalities are required for nodes that will need to communicate with nodes different from those that they were initially configured to trust. As a consequence, the trust level of a node's produced data/events must be measured/evaluated by the Trust Management enabler.	SAFECITY Communication Security Application	SAFECITY Communication Security Application	Trust Management	The Trust Management SE is responsible for establishing trust relationships and managing access lists and security profiles when a new node joins the network or for subscription to new services. The knowledge of when and where an event was triggered and/or measured can be used for extracting whether the transmitted information is trustworthy or not. Such a classification of information may define associated information protection requirements in terms of restricting the acceptance and circulation of produced data.	Trust plays an important role in IoT applications where the surrounding environment varies. Therefore, it is essential for the Security Manager to be able to verify that someone is who it claims to be and to determine if it is a legitimate member of the network. Such functionalities are required for nodes that will need to communicate with nodes different from those that they were initially configured to trust.