CITY.RISKS

AVOIDING AND MITIGATING SAFETY RISKS IN URBAN ENVIRONMENTS

Deliverable D2.4

Use Cases, Requirements and Key Performance Indicators

Editor P. Mehta (FUB)

Contributors P. Mehta **(FUB)**, N. Lehmann **(FUB)**

Version 1.2

Date August 31st, 2016

Distribution PUBLIC (PU)

GRANT AGREEMENT NO.653747

Executive Summary

This report documents the use case definition, requirements analysis and design of Key Performance Indicators conducted in the City.Risks project. It uses the survey of the state-of-the-art conducted previously in the project [1] to elaborate on scenarios where the adoption of modern technologies can assist in addressing security threats. Based on the outcomes of D2.2 [2] and D2.3 [3], emphasis has been laid on using citizen engagement in criminality detection and response, building communities to improve citizens' perception of security and to reduce their fear of crime, and using citizens' mobile devices and user generated content as tools for gaining insights into security threats and for addressing them more effectively. To ensure a diverse set of use cases, several target user groups, such as citizens, tourists, government authorities, and security services have been taken into account.

Each of the six defined use cases have been analyzed to produce a comprehensive set of technical requirements necessary for the development of the technical solutions in City.Risks. These have been separated into functional and non-functional requirements, where the functional requirements have been further grouped by the actor interacting with the platform and the architectural subsystem. The presented requirements will form the basis for the development of a final platform architecture in the upcoming stages of the project lifecycle.

Finally, a set of Key Performance Indicators (KPIs) for the evaluation of the performance, impact, and acceptance of the technical solutions have been defined. These criteria assess the performance of the system from various perspectives, including technical, social and psychological standpoints. Each KPI contains a well-defined set of attributes used for identifying and continuously monitoring and documenting the system's performance over time.

Table of Contents

1. Introduction

1.1. Scope

The main objective of this report is to present and describe the use cases, requirements and Key Performance Indicators (KPIs) for the City.Risks project against which the progress and the degree of fulfillment of the goals of the project can be measured. The focus lies on the mitigation and avoidance of urban crime not through the elimination of the actual threats, but rather by how individuals can act in order to minimise personal harm [2]. The proposed use cases employ modern technologies that can assist in preventing crime, in encouraging two-way communication between users and in increasing the perception of security within communities. They base themselves on the work already conducted in the project on the study of related platforms, state-of-the-art technologies, and open challenges and gaps in addressing security threats in urban settings [1]. Moreover, insights from the surveys assessing the factor affecting citizens' fear of crime [2] and from the study of different aspects of urban crime [3] conducted in the project have been utilized. The analysis and results show that although across the three pilot sites, the fear of becoming a victim of crime is high, the majority of the people own a smartphone and are willing to use it to report and share information about crimes via a mobile app. Another important insight is the role of public trust in the criminal justice system in reducing the fear of crime. Using the Operation Center component, criminal justice agencies can be a part in the development and the operation of the City.Risks platform. This would provide a direct link between the agencies and the citizens and can increase public confidence in the criminal justice system and in turn reduce the fear of crime.

The presented use cases encompass different target user groups and simulate diverse real-life situations in urban spaces in which the use of modern ICT technologies is beneficial. They have been designed to be in line with the City.Risks objectives of reducing the fear of crime among citizens, increasing their perception of security, fostering and facilitating information sharing in communities, engaging citizens in their local areas to act as *citizen sensors* using their mobile devices, and employing multiple data sources including user generated content for better understanding and responding to security threats.

The requirements for the project have been derived from the use cases and include the technical details of each use case from the perspective of different roles interacting with the platform. As a part of the requirements design process, the requirements for the architecture and functionality of the core platform and the mobile application were formulated. This will form the basis for the design of the architecture of the City.Risks platform. The requirements have been split into functional and non-functional, where the functional requirements have been further categorized based on the actor and the architecture subsystem involved in them, and the non-functional requirements have been classified based on the aspects they refer to.

The Key Performance Indicators have been derived from the use case definition and the requirements analysis. The KPIs give metrics for the evaluation of the performance, impact and acceptance of the technical solutions developed in the project. While designing the KPIs, emphasis has been laid on choosing a set of indicators that present a comprehensive picture of the performance of the project, both from technical as well as social and psychological standpoints.

1.2. Actors and Stakeholders

After discussing the scope of this report, we now present the actors that interact with the City.Risks platform and the stakeholders that are involved in or are affected by the project. The following are the stakeholders: *citizens*, *tourists*, *government institutions* such as city councils and municipalities, *safety and security services* such as the police force, fire department and private security agencies, the *City.Risks consortium members* who are involved in the development lifecycle of the platform, and *Small and Medium-sized Enterprises (SMEs)* who will be offering applications on top of the platform using the City.Risks SDK.

The requirements analysis presented in this document focuses on three main actors or roles that model the entities interacting with the platform. Each requirement describes an actor's interaction with the system. The following are the actors:

- **Mobile Application Users (MAU)**: The mobile application users include the citizens and visitors who would be using the City.Risks mobile application for staying informed about security conditions by receiving alerts and building communities and for serving as *citizen sensors* by reporting threats. The mobile application serves as a two-way communication channel between the mobile application users and the operation center.
- **Operation Center Users (OCU)**: This role represents the staff monitoring the City.Risks Operation Center. These include members of government bodies, such as city councils and municipalities. The Operation Center offers these users a tool for situational awareness, crisis management and response, and a platform for providing information to the safety and security services.
- **City.Risks system**: This role models the view of the City.Risks platform from its subsystems as technical actors. This allows us to formulate the functional and non-functional requirements based on the communication between platform subsystems and to model the information flow between these entities in each use case. It also allows us to group and categorize requirements according to the architectural subsystem to facilitate a modular design.

1.3. Requirements Analysis Methodology

Requirements analysis is a practice of software engineering concerned with the functions and constraints of a system. It involves coming up with set of precise specifications of behavior of the system [17]. The requirements analysis presented in this report is based on a set of specific methods for discovering the use cases and deriving the requirements and KPIs. Special emphasis was laid on artefact-based

methods and creative methods. The following methods were used to conduct the requirements analysis:

- **Literature research**: As mentioned earlier, existing work in City.Risks has identified challenges and gaps in security conditions in urban spaces by conducting a survey and analysis of existing solutions and technologies for addressing security challenges. The identified gaps and challenges were important considerations while defining the use case scenarios. Moreover, the surveyed solutions and technologies were analyzed while defining the scope and content of the use cases and requirements. This allowed us to come up with a broad-ranging set of use cases that meet the identified gaps and challenges.
- **Perspective-based reading**: While formulating the requirements based on the use cases, it is important to consider the views of the platform from the perspective of different actors. For this, we employed the technique of perspective-based reading [11]. Here, we tried to take turns in inspecting the use cases from the perspective of the different actors in the system with the goal of finding defective or omitted information.
- **Brainstorming**: Another important tool in the use cases and requirements design process was brainstorming about security challenges, scenarios, functionalities, target audience, etc. internally and with project partners at periodic progress meetings and conference calls.

1.4. Structure of the Deliverable

This document is structured into four main parts: Use cases, Draft System architecture, Requirements and Key Performance Indicators. Section 2 elaborates the City.Risks use cases by describing the actors involved, the goal, the flow and other attributes of each use case. An initial draft of the architecture for the City.Risks platform is presented in the next section, which is later used to subdivide functional requirements based on the architectural subsystem involved. Section 4 describes the requirements derived from the uses cases which are separated into functional and non-functional requirements. Next, the design and choice of suitable Key Performance Indicators for performance evaluation is presented. Finally, Section 6 concludes the report.

2. Use Cases

This section presents the six identified use cases of the City.Risks project. Each use case is described by explaining the order of events comprising it (main flow) and certain attributes, including the pre- and post-conditions, actors involved and exceptions. Each use case represents a collection of scenarios found in the previous analyses [1] [2] [3].

2.1. UC1: Theft of Personal Belongings

Theft of personal belongings, such as mobile devices, bags and bicycles, is an offence that is prevalent in most urban areas [16] [15], including the pilot sites of the project based on recorded crime figures and citizen survey findings [2]. The victims of the offence are citizens and unsuspecting visitors who not only lose their personal items of monetary value, but also things with an emotional and psychological value attached to them. It also affects the attractiveness of the destination [13]. Thus, tackling theft is an important challenge for any solution aiming to tackle crime and ensure security and safety in urban areas. This use case focuses on combating theft by using the potential of crowd sensing to locate a stolen item.

Main flow: A user's personal item gets stolen and the theft is reported to the Operation Center. The sensor stays in hibernation mode until activated. After receiving the theft report from the mobile application user (MAU), the theft detection sensor attached to the item is activated remotely from its hibernation mode via the Operation Center by multicasting a signal that triggers the sensor to periodically broadcast signals to mobile devices in proximity.

The signal broadcasted by the sensor is picked up by a mobile device with the City.Risks mobile application. The theft detection application on the mobile device runs in the background. The application notifies the Operation Center with its current location that the stolen item has been located. The Operation Center sends a notification to the security services, that the stolen item has been located, including its last located position.

Name	*Theft of personal belongings*
Identifier	*UC1*
Description	*A user's personal item gets stolen.*
Goal	*To locate a stolen item.*
Scope	*Tackling theft of personal belongings through crowd sensing.*
Preconditions	*A theft detection sensor, a small and discrete self-powered sensor based on Bluetooth Low Energy radio, is attached to the personal item.*

	The sensor is registered with the Operation Center.
Post conditions	*The location of the stolen item becomes known.*
Actors	*Mobile Application User, City.Risks system*
Exceptions	*The stolen device does not come in proximity of any mobile device with the City.Risks application.* *The sensor fails to get activated as it is out of range, out of battery or disabled by the offender.*

Table 1: UC1 description

2.2. UC2: Vehicle Theft

The second use case also deals with the common scenario of theft, but it concentrates on vehicle theft, including theft of cars and electric bicycles. It is the most prevalent form of crime in Rome according to official crime figures [2]. As in the previous use case, the solution used to tackle the problem is crowd sensing while focusing on specific groups of people, such as taxi drivers and petrol station employees.

Main flow: A vehicle is protected by two components: an inexpensive IoT device that is plugged in the cigarette lighter and a community-based Crowd-Sensing-Service in the City.Risks mobile application. The IoT device is capable of robustly detecting any manipulation attempt and movement of the vehicle. As soon as a manipulation or a non-authorized movement is detected, an alert is sent to the City.Risks mobile application of the owner who approves if this is a false alert or a real theft.

If a theft is confirmed by the owner, information about the vehicle is sent to other MAU and particular groups of people in an estimated reach area around the last known location of the vehicle. The alert radius is widened periodically by another ring of estimated reach probability. If an MAU detects the vehicle, she/he presses a button in the mobile application that immediately informs the Operation Center about the last detected position of the vehicle.

Name	*Vehicle theft*
Identifier	*UC2*
Description	*A user's vehicle, such as car or electric bike, gets stolen.*
Goal	*To locate a stolen vehicle.*
Scope	*Countering vehicle theft through crowd sensing.*
Preconditions	*A vehicle is equipped with an IoT device that is plugged into the cigarette lighter.* *The user has the City.Risks mobile application installed on her/his mobile device*

Post conditions	*The location of the stolen vehicle becomes known.*
Actors	*Mobile Application User, City.Risks system*
Exceptions	*The stolen vehicle is not detected by any MAU.* *The vehicle owner does not receive an intimation of the manipulation attempt.* *The IoT device fails to detect the manipulation attempt or is disabled by the offender.*

Table 2: UC2 description

2.3. UC3: Information Gathering and Dissemination for Ongoing Events

This use case targets scenarios involving large scale ongoing events, such riots, shootings and acts involving violence and unrest in public places. Such incidents tend to involve large gatherings or tend to occur in crowded urban areas and can have a high impact. Therefore, collecting information about the event as it unfolds and informing people at the scene on time becomes crucial. The citizens can serve as ground reporters and send current crime-related information to the Operation Center using their mobile phones, whereas the responsible authorities can act on this data and share information about their activities with the public using the Operation Center. This has the potential of increasing public trust in the criminal justice system and reducing fear of crime [2].

Main flow: MAU in a busy urban area witness an ongoing incident. They take pictures and capture videos of the situation and stream it in real-time to the Operation Center. The operation center user (OCU) uses the Operation Center to view maps of the area, reports about the incident from online sources and video streams of the incident from the citizens. Through the Operation Center, the OCU is able to relay information from authorities to citizens, provide information to other agencies and locate citizens in the vicinity who might be at risk.

Alerts and evacuation instructions are sent out to mobile devices of users in and near the affected area via the Operation Center. MAU who need assistance are recommended other trusted MAU offering help.

Name	*Information gathering and dissemination for ongoing events*
Identifier	*UC3*
Description	*Citizens witness an ongoing incident, such as a shooting or a riot, in a busy urban area.*
Goal	*To gather incident information and respond to the event.*

Scope	*Gathering and disseminating information regarding ongoing events involving large numbers of people.*
Preconditions	*Users at the scene of the incident have the City.Risks application installed on their mobile devices.*
Post conditions	*The OCU uses the Operation Center to view information about the incident from citizen users and online sources and to respond to the event.*
Actors	*Mobile Application User, Operation Center User, City.Risks system*
Exceptions	*The communication channels are taken down or become inactive.* *There are no users with City.Risks mobile application at the scene.*

Table 3: UC3 description

2.4. UC4: Tourists' and Women's Safety

Certain groups of people, such as tourists and visitors, women and ethnic minorities, can be at an elevated risk of victimization in comparison to other people [3]. The recorded levels of fear of crime also vary between different citizen groups and some of them, e.g., women, are more fearful of victimization than others [2]. Similarly, tourists might feel unsafe when visiting unfamiliar areas and could benefit from safety-related information [3]. Furthermore, as crime and victimization patterns generally vary with location and time, this use case deals with the task of equipping these groups of citizens with tools on their mobile devices for meeting their localized and temporal safety needs. This involves providing locally and temporally relevant information for allowing citizens to make informed decisions about their safety, e.g., safety-aware route planning depending on the area and the time of the day, informing a trusted network of people automatically when the user is at risk and providing ride sharing recommendations.

Main flow: Consider a citizen planning a journey to an unfamiliar city or walking home alone late at night. She/he may like information on the current level of crime in some parts of the city or specific information, such as the level of safety of women and ethnic minorities or the acceptance of LGBT people in the city.

She/he uses crime maps and augmented reality features of the City.Risks mobile application to view the crime levels by area and by category. She/he also tags items to bring them to others' notice.

While planning travel, she/he uses the safe routing functionality and the ride sharing recommendations of the mobile application to avoid unsafe areas or to find other MAU to accompany her/him during the journey.

The citizen also creates a group of people who should be informed when she/he might be unsafe. If the mobile application detects a situation involving high risk, depending

on the location, the time and other factors, it automatically informs the people in the MAU's trusted network.

Name	*Tourists' and women's safety*
Identifier	*UC4*
Description	*A citizen planning a journey to an unfamiliar city or walking home alone late at night.*
Goal	*To provide users information and tools for safety.*
Scope	*Providing users with safety-related information and services.*
Preconditions	*The user has the City.Risks mobile application installed on her/his mobile device.*
Post conditions	*The user stays safe and informed.*
Actors	*Mobile Application User, City.Risks system*
Exceptions	*The user does not find the information she/he seeks in the mobile application.*

Table 4: UC4 description

2.5. UC5: Citizen Engagement

With the advent of social media, widespread mobile devices and support for open governance, new avenues for engaging citizens with the activities in their surroundings have emerged. Citizen eye witnesses can often deliver important information that is not captured by dedicated infrastructure in cities [10]. This can go a long way in ensuring safety and security by addressing security challenges through information sharing between citizens and authorities. In addition, among the survey respondents in the pilot sites, the willingness to report and share information about crimes via smartphone apps was high [2]. This can also improve public trust and perception of security by reducing the time it takes to report a crime [2]. Thus, this use case focuses on equipping citizens with tools for reporting issues and suspicious activities in their area.

Main flow: An MAU is concerned about safety and order in her/his city. She/he would like to get information about past crime incidents in the city and wants to actively report issues. The MAU uses the mobile application to find past reports and statistics about incidents in different parts of the city using crime maps and explores crime-related data in her/his area using augmented reality in the mobile application.

Whenever the MAU finds a problem, she/he reports it by taking pictures, capturing videos, number plate information, etc. and sending it via the mobile application to the Operation Center.

Name	*Citizen engagement*
Identifier	*UC5*
Description	*A citizen wants to actively report issues.*
Goal	*To engage citizens in providing security-related information.*
Scope	*Equipping citizens with tools for reporting issues and threats.*
Preconditions	*The citizen has the City.Risks mobile application installed on her/his mobile device.*
Post conditions	*Citizens report issues and suspicious activities to the Operation Center.*
Actors	*Mobile Application User, City.Risks system*
Exceptions	*None*

Table 5: UC5 description

2.6. UC6: Neighborhood Safety

One of the important factors contributing to the perception of security among citizens is the sense of belonging to a community. Most people already use mobile phones for sharing information via social networking and instant messaging applications [2]. In addition, collaborative and community-based approaches to alerting enable citizen participation and transparency in the event of an incident occurrence [9]. Thus, fostering and facilitating information sharing in communities and trusted networks is a key objective of the City.Risks project. This is also the focus of this use case.

Main flow: A group of MAU living in the same neighborhood use the mobile application to create communities through which they stay informed about situations that can affect the security in the neighborhood.

Individual MAU can subscribe to communities of interest and notify the other members about important situations and incidents affecting the safety of the neighborhood, e.g., suspicious activity in the area or a break-in attempt, so that other MAU can take countermeasures to stay secure.

If an MAU becomes a victim of an offence, such as vandalism of personal property or hate crime, she/he can use the mobile application to submit a request for witnesses who were near the crime scene around the time it happened. MAU in the victim's network who were nearby at the time of the incident, send back photos of the culprits. The images are used to report the incident.

Name	*Neighborhood safety*
Identifier	*UC6*

Description	*Citizens build communities for sharing safety-related information.*
Goal	*To foster and facilitate information sharing between citizens.*
Scope	*Addressing security challenges by fostering and facilitating information sharing in communities.*
Preconditions	*Multiple citizens have the City.Risks mobile application installed on their mobile devices.*
Post conditions	*Citizens build online communities and exchange safety-related information in them.*
Actors	*Mobile Application User, City.Risks system*
Exceptions	*None*

Table 6: UC6 description

3. Draft System Architecture

Based on the use case description presented in the last section, a draft of the architecture of the City.Risks platform is presented below in Figure 1. As shown, it is a layered architecture comprising three layers – the Access layer, the Application layer and the Resource and Data layer, each containing multiple components. This is an initial draft only, as the design of the final platform architecture is the scope of a separate project deliverable (D2.5).

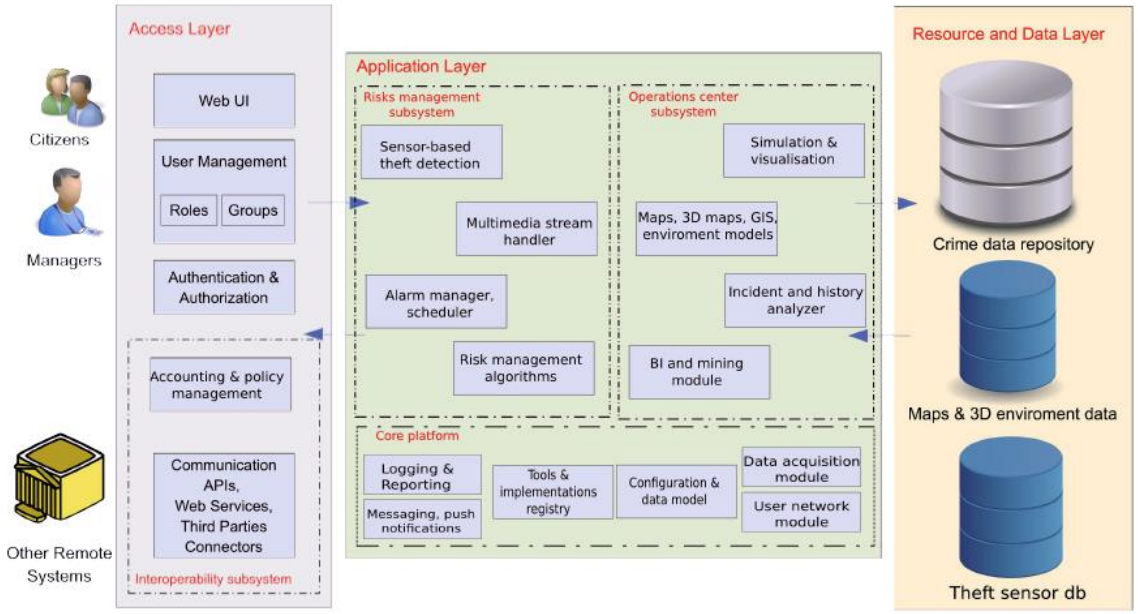


Figure 1: City.Risks draft platform architecture

The requirements presented in the following section have been grouped by the architecture subsystems and divided into functional and non-functional requirements. The three components: Web UI, User Management and Accounting and Policy Management, in the Access Layer are grouped into the Web Portal subsystem. Also, in addition to the three layers shown in Figure 1, an additional layer, called the Remote layer, is used for mapping the requirements to subsystems. The Remote layer consists of two subsystems, namely the mobile application and the theft detection subsystem (theft detection sensors and IoT devices). Below is a list of the architecture subsystems and their components by layer:

1. Access Layer

   Web Portal subsystem

   - Web UI
   - User Management (Roles, Groups)
   - Authentication & Authorization

   Interoperability subsystem

   - Accounting & policy management
   - Communication APIs, Web Services, Third Parties Connectors

2. Application Layer

   Risks Management subsystem

   - Sensor-based theft detection module
   - Multimedia stream handler
   - Alarm manager, scheduler
   - Risk management algorithms

   Operation Center subsystem

   - Simulation & visualization module
   - Maps, 3D maps, GIS environment models
   - Incident and history analyzer
   - BI and mining module

   Core Platform subsystem

   - Logging & reporting module
   - Messaging, push notification module
   - Tools & implementations registry
   - Configuration & data model
   - Data acquisition module
   - User network module

3. Resource and Data Layer
   - Crime data repository
   - Maps & 3D environment data
   - Theft sensor DB
4. Remote Layer
   - Mobile application
   - Theft detection subsystem

4. Requirements

In this section, the requirements for the City.Risks platform generated from the use case definition are described. Each requirement entry therefore lists the use cases that it is related to. The overall set of requirements is classified into two categories: functional and non-functional. The functional requirements have been further subdivided based on the involved actor and the architectural subsystem (described in the last section), whereas the non-functional requirements are grouped by the non-functional aspects they describe, including security and privacy, scalability, performance, reliability and availability, and manageability and flexibility.

Category: R1 Functional Requirements		
Group 1: Actor - Mobile Application User (MAU)		
Code	**Description**	**Relevant Use Cases**
R1.1.1	An MAU is able to create and edit her/his profile with personal information and preferences, including rules and policies for sharing information.	All
R1.1.2	An MAU is able to create and send an incident report to the Operation Center.	All
R1.1.3	An MAU is able to receive location-based notifications, including warnings and alerts.	UC2, UC3, UC4, UC6
R1.1.4	An MAU is able to capture and send multimedia content, such as audio, video and images, via the mobile application to the Operation Center subsystem.	UC3, UC5, UC6
R1.1.5	An MAU is able to view crime statistics by location, time and type on a map.	UC4, UC5
R1.1.6	An MAU is able to view safety indicators for an area, e.g., safety levels for women, LGBT citizens or ethnic minorities.	UC4, UC5
R1.1.7	An MAU is able to use augmented reality to view the crime-related information about her/his surroundings.	UC4, UC5
R1.1.8	An MAU is able to interact with objects presented in augmented reality, i.e., add information to objects, update objects and create new objects.	UC4, UC5
R1.1.9	An MAU is able to register a theft detection sensor with the Operation Center.	UC1

R1.1.10	An MAU is able to report a theft to the Operation Center via the mobile application.	UC1
R1.1.11	An MAU is able to reject or confirm a received vehicle theft notification.	UC2
R1.1.12	An MAU is able to inform the Operation Center about the sighting of a stolen vehicle.	UC2
R1.1.13	An MAU is able to notify the Operation Center subsystem about the need for help.	UC3
R1.1.14	An MAU is able to create a trusted network who will be informed when she/he might be in danger.	UC4
R1.1.15	An MAU is able to receive personalized and visualized risk information about an area through updates, maps and mAR based on their profile, location, time and preferences.	UC4
R1.1.16	An MAU is able to search for routes between two locations on a map.	UC4
R1.1.17	An MAU is able to view safety related information on routes between two locations on a map.	UC4
R1.1.18	An MAU is able receive ride sharing recommendations from the Operation Center.	UC4
R1.1.19	An MAU is able to send requests for ride sharing recommendations to the Operation Center.	UC4
R1.1.20	An MAU is able to report problems and complaints, such as illegal dropping of waste and illegal business activity, to the Operation Center subsystem.	UC5
R1.1.21	An MAU is able to create communities.	UC6
R1.1.22	An MAU is able to join an existing community or leave an existing community that she/he is a member of.	UC6
R1.1.23	An MAU is able to post text messages in the community that she/he is a part of.	UC6
R1.1.24	An MAU is able to post multimedia files, such as images, audio and videos, in the community that she/he is a part of.	UC6
R1.1.25	An MAU is able to send requests for witnesses to the Operation Center subsystem with the incident location and time.	UC6

R1.1.26	An MAU is able to specify a storage limit for her/his history of locations and timestamps on the mobile device.	UC6
R1.1.27	An MAU is able to receive requests for witnesses by the Operation Center subsystem.	UC6
R1.1.28	An MAU is able to confirm or reject requests for witnesses from the Operation Center subsystem.	UC6
Group 2: Actor – Operation Center User (OCU)		
R1.2.1	An OCU is able to keep track of ongoing incidents using map and text-based interfaces.	UC3
R1.2.2	An OCU is able to filter event information based on event attributes, such as location and time.	UC3
R1.2.3	An OCU is able to aggregate event information from different sources.	UC3
R1.2.4	An OCU is able to visualize event information over a map.	UC3
R1.2.5	An OCU is able to send a common notification, such as an alert or a warning, to a specific subset of recipients based on their location.	UC3
R1.2.6	An OCU is able to view reports of an incident over a map.	UC3
R1.2.7	An OCU is able to locate MAU within a specific range of an incident occurrence.	UC3
R1.2.8	An OCU is able to send advisories and instructions to MAU based on their location.	UC3
R1.2.9	An OCU is able to simulate different scenarios for planning and preparedness, e.g., using agent-based simulations.	UC3
Group 3: Access Layer – Web Portal Subsystem		
R1.3.1	The Web Portal subsystem can provide an interface to create and edit user profile with personal information and preferences, including rules and policies for sharing information.	All
R1.3.2	The Web Portal subsystem can display crime statistics by location, time and type on a map.	All
R1.3.3	The Web Portal subsystem can allow the registration of a theft detection sensor with the Operation Center.	UC1

R1.3.4	The Web Portal subsystem can provide an interface to create communities.	UC6
R1.3.5	The Web Portal subsystem can allow a user to join an existing community or leave an existing community that she/he is a member of.	UC6
R1.3.6	The Web Portal subsystem can allow a user to post text messages in the community that she/he is a part of.	UC6
R1.3.7	The Web Portal subsystem can allow a user to post multimedia files, such as images, audio and videos, in the community that she/he is a part of.	UC6
Group 4: Access Layer – Interoperability Subsystem		
R1.4.1	The Interoperability subsystem can enable program-to-program interoperability using an API and open web standards-based protocols (e.g. HTTP, SOAP, XML, etc.).	All
R1.4.2	The Interoperability subsystem can allow a third-party application to access and query data to provide additional features on top of the City.Risks platform.	All
Group 5: Application Layer – Operation Center Subsystem		
R1.5.1	The Operation Center subsystem is able to provide specific crime-related structured data to the security services via a REST API based on parameters like time period, area or type.	All
R1.5.2	The Operation Center subsystem is able to extract contextual data about an incident from web sources.	UC3, UC4
R1.5.3	The Operation Center subsystem is able to activate a theft detection sensor remotely by generating and sending a wake-up signal.	UC1
R1.5.4	The Operation Center subsystem is able to broadcast information about a stolen vehicle to MAU within a specific range around the last known location of the vehicle.	UC2
R1.5.5	The Operation Center subsystem is able to send information about a vehicle to specific groups of MAU.	UC2
R1.5.6	The Operation Center subsystem is able to determine an estimate reach area around the last location of a vehicle based on time.	UC2

R1.5.7	The Operation Center subsystem is able to re-estimate the reach area around the stolen area with time.	UC2
R1.5.8	The Operation Center subsystem is able to provide MAU information about persons near them who need help.	UC3
R1.5.9	An MAU is able to report situations involving risk and information about risk at a location to the Operation Center subsystem.	UC4
Group 6: Application Layer – Risks Management Subsystem		
R1.6.1	The Risks Management subsystem is able to track the position of an MAU.	UC3, UC4
R1.6.2	The Risks Management subsystem is able to monitor MAU near a specific MAU.	UC3, UC4
R1.6.3	The Risks Management subsystem is able to monitor static (maps, crime statistics) and real-time (current events and conditions) data about a location.	UC3, UC4
R1.6.4	The Risks Management subsystem is able to supply an MAU at risk with situation-aware personalized information and advisories on how to respond.	UC3, UC4
R1.6.5	The Risks Management subsystem is able to send warnings and alerts to a certain MAU or a group of MAU based on location.	UC3
R1.6.6	The Risks Management subsystem is able to aggregate and visualize event-related information.	UC3
R1.6.7	The Risks Management Subsystem is able to mine patterns, such as hotspots and seasonality, using internal and external crime-related and contextual data.	UC4
R1.6.8	The Risks Management subsystem is able to find ride sharing recommendations for a user.	UC4
Group 7: Application Layer – Core Platform Subsystem		
R1.7.1	The Core Platform subsystem can enable a third-party to build and integrate a custom application into the City.Risks platform using the SDK.	All
R1.7.2	The Core Platform can provide low level system monitoring and event logging.	All
R1.7.3	The Core Platform subsystem is able to provide an infrastructure for managing user communities, e.g.,	UC6

	creating communities and updating community memberships.	
R1.7.4	The Core Platform subsystem is able to provide an infrastructure for managing community policies, e.g., roles and access.	UC6
Group 8: Resource and Data Layer		
R1.8.1	The Resource and Data Layer is able to add, update and provide data through an API.	All
R1.8.2	The Resource and Data layer is able to access and update different types of content from different data sources. This includes: ▪ crime reports and statistics ▪ geospatial data (maps) ▪ demographic data ▪ 3D environment data (if available) ▪ multimedia data (audio, video, images) ▪ theft detection sensor registration data (sensor registry) ▪ applications and services registration data (tools registry) ▪ user IDs, user profiles, user groups and roles (user registry)	All
R1.8.3	The Resource and Data layer is able to support different types of attribute-based queries.	All
R1.8.4	The Resource and Data Layer is able to support different types of analysis (i.e., offline, real-time and continuous).	All
Group 9: Remote Layer – Mobile Application		
R1.9.1	The mobile application is able to communicate with the Operation Center subsystem over wireless interfaces.	All
R1.9.2	The mobile application is able to identify a specific theft detection sensor or IoT device, i.e., a sensor or IoT device attached to an item/vehicle that was stolen	UC1, UC2
R1.9.3	The mobile application is able to provide a dynamic, high-performance, cloud-based and OGC-conforming Web Processing Service (WPS) for generating and providing dynamic mobile Augmented Reality (mAR) representations in real-time.	UC4, UC5

R1.9.4	The mobile application provides an interface for rendering, generating and modifying content based on the mAR data description language.	UC4, UC5
R1.9.5	The mobile application is able to interact with the mAR WPS for generating and displaying dynamic mAR representations in real-time.	UC4, UC5
R1.9.6	The mobile application is able to display safety and risk information in the mAR view of the mobile device.	UC4, UC5
R1.9.7	The mobile application is able to communicate with theft detection sensors via a proximity-based mechanism.	UC1
R1.9.8	The mobile application is able to receive a short-range signal from a theft detection sensor.	UC1
R1.9.9	The mobile application is able to send a notification with the position, time and ID of a nearby theft detection sensor to the Operation Center.	UC1
R1.9.10	The mobile application is able to receive vehicle theft notification from an IoT device.	UC2
R1.9.11	The mobile application is able to send vehicle theft information to the Operation Center.	UC2
R1.9.12	The mobile application is able to poll the Operation Center subsystem for cases that require witnesses.	UC6
R1.9.13	The mobile application is able to evaluate based on location history if it was in the spatial and temporal range of an incident.	UC6
R1.9.14	The mobile application is able to send a confirmation to the Operation Center subsystem only after the MAU has verified that she/he would like to act as a witness in the case.	UC6
Group 10: Remote Layer – Theft Detection Subsystem		
R1.10.1	The theft detection sensor is able to function for a long time period without an external power source.	UC1
R1.10.2	The theft detection sensor can be attached to a personal item, such as handbag, luggage or bicycle.	UC1
R1.10.3	The theft detection sensor is able to communicate with the mobile application using Bluetooth Low Energy radio.	UC1
R1.10.4	The theft detection sensor is able to broadcast a signal periodically to mobile devices in proximity.	UC1

R1.10.5	The theft detection sensor is able to go into hibernation mode.	UC1
R1.10.6	The theft detection sensor is able to get activated by a remote signal from the Operation Center subsystem.	UC1
R1.10.7	The IoT device can be attached to the cigarette lighter in a vehicle.	UC2
R1.10.8	The IoT device is able to detect any manipulation or movement of the vehicle it is attached to.	UC2
R1.10.9	The IoT device is able to send an alert to the mobile application of the owner of the vehicle the IoT device is attached to.	UC2
Category: R2 Non-Functional Requirements		
Group 1: Security and Privacy		
Code	**Description**	**Relevant Use Cases**
R2.1.1	The theft detection sensor is small enough in size to be attached and hidden with a personal item, such as a handbag.	UC1
R2.1.2	The theft detection sensor cannot be easily disabled by an unauthorized person once it is activated by the Operation Center.	UC1
Group 2: Scalability		
R2.2.1	The Operation Center subsystem can handle sudden bursts in incoming traffic volume.	All
R2.2.2	The Operation Center subsystem can handle a large number of requests simultaneously.	All
R2.2.3	The Resource and Data Layer is able to manage large volumes of different types (geospatial, multimedia, crime, sensor, user, etc.) of data.	All
Group 3: Performance		
R2.3.1	The Operation Center has a low response time to incoming requests.	All
R2.3.2	The theft detection service should run in the background in the mobile application in a single thread.	UC1
Group 4: Reliability and Availability		

R2.4.1	The theft detection sensor is self-powered and can last without a power source for a long period of time.	UC1
R2.4.2	The responsiveness of the mobile application should not be affected by the operation of the theft detection background service.	UC1
Group 5: Manageability and Flexibility		
R2.5.1	The mobile application, Operation Center and Web Portal interfaces are is user-friendly.	All
R2.5.2	The theft detection sensor and IoT device are inexpensive.	UC1, UC2
R2.5.3	The theft detection sensor is easy to attach to an item or detach from an item.	UC1
R2.5.4	The registration of theft detection sensor with the Operation Center is user-friendly and straightforward.	UC1

5. Key Performance Indicators

5.1. Usage of Key Performance Indicators

In the pilot phase (WP6), the performance of the City.Risks approach will be validated and evaluated by setting up and conducting pilot trials at multiple sites in Europe. The success of the project will be determined not only by the performance, impact and acceptance of the technical solution, but also by its psychological and social impact. Therefore, a mechanism for enabling continuous evaluation of the pilot deployments through measurement of a set of indicators or metrics is needed. To this end, in this section, the design of suitable Key Performance Indicators (KPI) is described based on existing literature [5][18] and a list of KPI is presented that fit into the context of the project.

5.2. Design of Key Performance Indicators

Below we present our choice of design of KPIs that fit the context of the project. Each KPI has ten attributes and its value is measured against its target value. The following are the attributes:

- **Name**: The name is a unique alphanumeric combination to identify the KPI.
- **Type**: The type describes how the KPI is designed, i.e. as a numeric value, an ordinal scale or a ratio scale.
- **Range/Scale**: The range delineates the range of values that the KPI can take on. For example, for a numeric KPI, the range would include a minimum and a maximum value, whereas for an ordinal scale KPI, this would be the range of possible values that the KPI can take on.
- **Weight**: The weight is a numeric value that expresses the importance of this KPI. The higher the value, the more important the KPI. The value of weight goes from 1 (interesting) through 2 (important) to 3 (very important).
- **Status**: This attribute shows in a simple visual manner the status of the measured item using color. The color green represents a positive status, the color yellow represents an average status and the color red represents a negative status.
- **Trend**: The trend attribute describes the estimated progress of the measured item visually. The chosen representation is an arrow that can point upwards, horizontally or downwards.
- **Actual Value**: The actual value shows the current value of a measured item.
- **Target Value**: The target value represents the desired value at the end of the measurement period.
- **Deviation**: The deviation in measurement is calculated as follows:
$$deviation = target\ value - actual\ value$$
- **Deviation in Percentage**: Similar to deviation, the deviation in percentage can be calculated as follows:
$$deviation\ in\ \% = \frac{target\ value - actual\ value}{target\ value}$$

5.3. List of Key Performance Indicators

After describing the structure of the KPIs, in the following a list of Key Performance Indicators chosen based on the use case design and requirements analysis is presented.

5.3.1. KPI1: Fear of Crime

5.3.1.1. Description

Fear of crime is important to include as a KPI because it is a distinct phenomenon from actual crime rates due to its highly subjective content [7] [6]. This KPI measures fear of crime among the users before, during, and after the implementation of the end user product.

In City.Risks, fear of crime will be evaluated by both quantitative and qualitative methodologies, through the use of targeted questionnaires, surveys and focus groups at the pilot sites, and by monitoring social media for fear of crime-related indicators. The mobile application uses a set of simple and easily comprehensible questions to gauge the level of fear of crime of users. The questions are posed to the users during the first use of the app to form a baseline for evaluation and periodically (once a month) from there on. The users (citizens) use an ordinal scale to answer the questions.

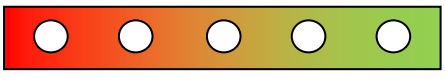
Since the fear of crime differs depending on the offence, this KPI will be crime-specific and will show a set of indicators as per the design below, one per crime type. This will also allow a more fine-grained analysis. At this stage, it is planned to focus on two specific crime types: violent crime and property crime, while this approach can be extended to other types of crime in the future. The following are the questions for the above two types, respectively:

"I fear becoming a victim of a violent crime."

"I fear becoming a victim of a property crime."

As this KPI and the other similar KPIs are to be evaluated every month, the above questions explicitly state this advance in order to receive correct and accurate responses. For instance, a statement like “These statements concern your perception of safety during the last month” would be posted before the start of the questionnaire.

The answering scale has five entries starting from "Highly agree", through "Somewhat agree", "Neutral", "Somewhat disagree" to "Highly disagree". Additionally, the ordinal scale presents a color gradient from red to green on the scale to allow the respondents to visually and intuitively voice his emotion. An illustration of the scale is shown below:



The weight of this KPI is 3 (very important).

5.3.1.2. KPI design

- name: fear_of_crime
- type: ordinal scale
- range/scale: five entries
  - strong negative value = "Highly agree"
  - negative value = "Somewhat agree"
  - neutral value = "Neutral"
  - positive value = "Somewhat disagree"
  - strong positive value = "Highly disagree"
- status:
  - red = "Highly agree" (high fear level)
  - yellow = “Somewhat agree”, "Neutral" (average fear level)
  - green = "Somewhat disagree", “Highly disagree” (low fear level)
- trend:
  - arrow down = positive
  - arrow horizontal = neutral
  - arrow up = negative
- target value: "Somewhat disagree"

5.3.2. KPI2: Perception of Security

5.3.2.1. Description

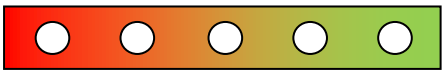
In difference from the previous KPI, this KPI is centered on the users’ perceptions of safety without any explicit connection to crime. This KPI thus embraces the common finding in criminological research that subjective perceptions of safety are contingent upon other factors than actual exposure to crime, such as, for instance, social and physical disorder [4][7], and neighborhood characteristics [7][8][14].

Perception of security is measured before, during, and after the implementation of the mobile application. The outcomes of the surveys, focus group meetings and social media monitoring will be used for a comprehensive assessment of the factors that can help to build a perception of security among citizens. To assess the perceived level of safety, the mobile application presents a set of questions to users during their first use of the app and once a month, subsequently. Similar to KPI1, this KPI is context-dependent and therefore will present a set of context-specific values, instead of one value. The mobile application users use an ordinal scale to answer the questions. Below is an example of two such questions:

"I feel safe walking alone in my local area during the day."

"I feel safe walking alone in my local area after dark."

The answering scale has five entries starting from "Highly disagree", through "Somewhat disagree", "Neutral", "Somewhat agree" to "Highly agree". The ordinal scale also presents a visual color gradient similar to the one shown below from red to green on the scale:



The weight of this KPI is 3 (very important).

5.3.2.2. KPI Design

- name: perception_of_security
- type: ordinal scale
- range/scale: 5 entries
  - strong negative value = "Highly disagree"
  - negative value = "Somewhat disagree"
  - neutral value = "Neutral"
  - positive value = "Somewhat agree"
  - strong positive value = "Highly agree"
- status:
  - red = "Highly disagree"
  - yellow = "Somewhat disagree", "Neutral"
  - green = "Somewhat agree", "Highly agree"
- trend:
  - arrow down = negative
  - arrow horizontal = neutral
  - arrow up = positive
- target value: "Somewhat agree"

5.3.3. KPI3: Involvement with Other People in Local Area

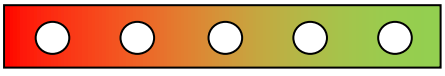
5.3.3.1. Description

Social cohesion refers to a person's feeling of belonging to a wider community. Low social cohesion in neighborhoods is related to both higher levels of fear of crime [4] [7] and high crime rates [12]. Measuring people's interactions in their home areas may reveal individuals' attachment to their local areas.

This KPI uses questionnaires to ask citizens if they believe that the City.Risks platform has facilitated their interactions with other citizens. The mobile application users use an ordinal scale to answer a simple question once a month:

"I have a lot of contact with other people in my local area."

The scale again has 5 entries starting from "Highly disagree", through "Somewhat disagree", "Neutral", "Somewhat agree" to "Highly agree". The ordinal scale also presents a visual color gradient from red to green like the one shown below:



The weight of this KPI is 3 (very important).

5.3.3.2. KPI design

- name: involvement_with_other_people_in_local_area
- type: ordinal scale
- range/scale: five entries
  - strong negative value = "Highly disagree"
  - negative value = "Somewhat disagree"
  - neutral value = "Neutral"
  - positive = "Somewhat agree"
  - strong positive value = "Highly Agree"
- status:
  - red = "Highly disagree"
  - yellow = "Somewhat disagree", "Neutral"
  - green = "Somewhat agree", "Highly Agree"
- trend:
  - arrow down = negative
  - arrow horizontal = neutral
  - arrow up = positive
- target value: "Somewhat agree"

5.3.4. KPI4: Number of Participants

5.3.4.1. Description

The next KPI measures the coverage of the evaluation in the terms of the number of participants. This includes the total number of participants (citizens, governmental staff, etc.) using the platform in the pilots.

The weight of this KPI is 2 (important).

5.3.4.2. KPI design

- name: number_of_participants
- type: integer values
- range/scale: integer values
  - minimum value = 0
  - maximum value = ∞
- status:
  - red = < 34% of the target value
  - yellow = 34% - 66% of the target value
  - green = > 66% of the target value
- trend:
  - arrow down = NA
  - arrow horizontal = negative
  - arrow up = positive
- target value: 750 users

5.3.5. KPI5: Frequency of Usage

5.3.5.1. Description

The frequency of usage KPI shows a weekly estimate of how frequently the platform is used by users (government authorities and citizens). On the mobile device this is estimated by keeping track each time the City.Risks mobile application is started (brought to the foreground of the device screen). The Operation Centre measures this through the logins into the interface.

The weight of this KPI is 3 (very important).

5.3.5.2. KPI Design

- name: frequency_of_usage
- type: integer values
- range/scale: integer values
  - minimum value = 0
  - maximum value = ∞
- status:
  - red = < 3 users per week (low frequency)
  - yellow = 4 - 6 users per week (average frequency)
  - green = > 6 users per week (high frequency)
- trend:
  - arrow down = negative
  - arrow horizontal = positive
  - arrow up = positive
- target value: 8 users a week

5.3.6. KPI6: Number of Incident Reports

5.3.6.1. Description

This KPI is based on the number of incident reports recorded by the City.Risks platform over the project duration. It is measured by counting all incident reports received by the Operation Center.

The weight of this KPI is 2 (important).

5.3.6.2. KPI Design

- name: number_of_incident_reports
- type: integer values
- range/scale: integer values

    - minimum value = 0
    - maximum value = ∞
- status:
    - red = < 50 reports
    - yellow = 50 - 99 reports
    - green = > 99 reports
- trend:
    - arrow down = NA
    - arrow horizontal = negative
    - arrow up = positive
- target value: 150 reports

5.3.7. KPI7: Frequency of Incident Reports

5.3.7.1. Description

The frequency of incident reports measures the number of incidents reports received per week by the Operation Center.

The weight of this KPI is 3 (very important).

5.3.7.2. KPI design

- name: frequency_of_incident_reports
- type: integer value
- range/scale: integer values
    - minimum value = 0
    - maximum value = ∞
- status:
    - red = < 1 reports per week (low frequency)
    - yellow = 1 - 2 reports per week (average frequency)
    - green = > 2 reports per week (high frequency)
- trend:
    - arrow down = negative
    - arrow horizontal = neutral
    - arrow up = positive
- target value: 3 reports a week

5.3.8. KPI8: Level of Engagement of Citizens

5.3.8.1. Description

This KPI estimates the level of engagement of citizens in security conditions in their area by calculating the portion of participants who have submitted content via the

City.Risks platform. The content could include instances like incident reports, video streams and community posts over the entire project duration.

The weight of this KPI is 3 (very important).

5.3.8.2. KPI Design

- name: level_of_engagement
- type: ratio scale
- range/scale: 1% increments
  - minimum value = 0% of all users (0 users)
  - maximum value = 100% of all users (750 users)
- status:
  - red = < 34% of all users
  - yellow = 34% - 66% of all users
  - green = > 67% of all users
- trend:
  - arrow down = NA
  - arrow horizontal = negative
  - arrow up = positive
- target value: 100% of all users (750 users)

5.3.9. KPI9: Number of Communities

5.3.9.1. Description

This KPI aims at estimating the success of the project at facilitating building of trusted networks and communities for improving information sharing and the perceived level of security among citizens.

The weight of this KPI is 2 (important).

5.3.9.2. KPI Design

- name: number_of_communities
- type: integer values
- range/scale: integer values
  - minimum value = 0
  - maximum value = ∞
- status:
  - red = < 2 communities
  - yellow = 2 – 4 communities
  - green = > 4 communities
- trend:
  - arrow down = negative
  - arrow horizontal = neutral

        - arrow up = positive
    - target value: 6 communities

5.3.10. KPI10: Mean Size of Communities

5.3.10.1. Description

This KPI measures the mean size of communities to give an indication of the reach or the extent of the networks created through the project.

The weight of this KPI is 1 (interesting).

5.3.10.2. KPI design

- name: mean_size_of_communities
- type: integer values
- range/scale: integer values
    - minimum value = 1
    - maximum value = ∞
- status:
    - red = < 3 users
    - yellow = 3 - 6 users
    - green = > 6 users
- trend:
    - arrow down = negative
    - arrow horizontal = neutral
    - arrow up = positive
- target value: 10 users

6. Conclusions

In this report, we presented the use cases, requirements and KPIs for the City.Risks project. The analysis described here follows the work conducted previously in the project on the study of gaps and challenges for addressing security threats in urban environments. We started with the definition of the set of use cases that the development of the platform will be based on. The goal of the use case definition was to come up with a diverse set of scenarios covering different target user groups and security conditions that can benefit from the integration of modern technologies. We have strived to ensure that the use cases go in the direction of fulfilling the objectives of the project, namely, reducing the fear of crime in citizens, increasing their perception of security, facilitating information exchange in user communities, engaging citizens in their local areas to act as *citizen sensors* using their mobile devices and taking a data-centric approach towards understanding and responding to security threats. Based on this, the following use cases have been defined: Theft of Personal Belongings, Vehicle Theft, Information Gathering and Dissemination for Ongoing Events, Tourists' and Women's Safety, Citizen Engagement and Neighborhood Safety.

The use case definition was used to extract the functional and non-functional requirements for the platform. These will lay the foundations for the design of platform architecture. The functional requirements have been grouped together based on the actor and the architectural subsystem involved in them and the non-functional requirements have been categorized based on the characteristics they relate to. The identified actors include mobile application users (citizens, tourists), Operation Center users (government staff monitoring the Operation Center) and the City.Risks system including its subsystems (Core Platform subsystem, Risks Management Subsystem, etc.).

Finally, the use case definition and requirements analysis was used to derive a set of Key Performance Indicators for evaluating the performance of the project starting from the pilot phase. These KPIs measure the success of the project from both technical, as well as social and psychological perspectives. The following set of KPIs have been defined: Fear of Crime, Perception of Security, Involvement with Other People in Local Area, Number of Participants, Frequency of Usage, Number of Incident Reports, Frequency of Incident Reports, Level of Engagement of Citizens, Number of Communities and Mean Size of Communities. Each KPI has its own weight to specify the importance of the indicator. Moreover, other than name and weight, each KPI has several other attributes, including type, actual value, target value, variance, percentage variance, trend, status and range.

References

[1] City.Risks Consortium. (2015). Deliverable D2.1 - Gaps and challenges for addressing security threats in urban environments. Retrieved from http://www.cityrisks.eu/deliverables/

[2] City.Risks Consortium. (2015). Deliverable D2.2 - Analysing factors influencing the fear of crime from the citizens' perspective. Retrieved from http://www.cityrisks.eu/deliverables/

[3] City.Risks Consortium. (2015). Deliverable D2.3 - Fine-grained analysis of security threats in large urban environments. Retrieved from http://www.cityrisks.eu/deliverables/

[4] Ditton, J. & Innes, M. (2005). The role of perceptual intervention in the management of crime fear. In: N. Tilley (ed.) *Handbook of crime prevention and community safety*. Cullompton, Devon: Willan Pub. pp. 595-623

[5] Eckerson, W. W. (2009). Performance management strategies. Business Intelligence Journal, 14(1), 24-27.

[6] Ferraro, K. F. (1995). *Fear of crime: interpreting victimization risk*. Albany, NY: State University of New York Press

[7] Farrall, S., Jackson, J. & Gray, E. (2009). *Social order and the fear of crime in contemporary times*. Oxford: Oxford University Press

[8] Hale, C. (1996). Fear of crime: a review of the literature. *International Review of Victimology*, 4 (2), pp. 79-150

[9] Lorenzi, D., Vaidya, J., Chun, S., Shafiq, B., Naik, V., Atluri, V., & Adam, N. (2013, June). Community based emergency response. In Proceedings of the 14th Annual International Conference on Digital Government Research (pp. 82-91). ACM.

[10] Roitman, H., Mamou, J., Mehta, S., Satt, A., & Subramaniam, L. V. (2012, November). Harnessing the crowds for smart city sensing. In Proceedings of the 1st international workshop on Multimodal crowd sensing (pp. 17-18). ACM.

[11] Shull, F., Rus, I., & Basili, V. (2000). How perspective-based reading can improve requirements inspections. *Computer*, *33*(7), 73-79.

[12] Sampson, R. J., Raudenbush, S. W., & Earls, F. (1997). Neighborhoods and violent crime: a multilevel study of collective efficacy. *Science*, 277 (5328), pp. 918-924

[13] The Guardian. Rome mayor hits back at Foreign Office warning over pickpockets. http://www.theguardian.com/world/2014/aug/17/rome-mayor-foreign-office-pickpockets-tourists. Accessed November 26, 2015.

[14] Tseloni, A. (2007). Fear of crime, perceived disorders and property crime. In: G. Farrell, K. Bowers, S. D. Johnson & M. Townsley (eds.) *Imagination for crime prevention: essays in honour of Ken Pease*. Crime prevention studies, vol. 21. Monsey, NY: Criminal Justice Press, pp. 163-185

[15] The Local de. (2014). Germany's Vicious Cycle of Bike Thefts. http://www.thelocal.de/20140717/germanys-vicious-cycle-of-bike-thefts. Accessed November 25, 2015.

[16] TripAdvisor. (2009). Top Ten Cities to be Beware of Pickpockets. http://www.tripadvisor.co.uk/PressCenter-i3309-c1-Press_Releases.html. Accessed November 25, 2015.

[17] Van Lamsweerde, A. (2009). Requirements engineering: from system goals to UML models to software specifications.

[18] Zehnter, C., Burger, A., & Ovtcharova, J. (2012). Key-Performance-Analyse von Methoden des Anforderungsmanagements (Vol. 7620). KIT Scientific Publishing.