SECUR-ED
SECured URban transportation - European Demonstration

D46.2 REPORT ON CONSOLIDATION OF FUNCTIONAL RESULTS

Document identification			
Related SP / WP	SP4 / WP46	**Reference**	SCR-WP46-D-ANS-003
Related Deliverable	D46.2-6	**Dissemination Level**	PUBLIC
Lead Participant	Ansaldo STS	**Lead Author**	Ansaldo STS
Contributors	ICCA, ALSTOM, ANSALDO, ATM, CTRM, DB, FNM, RATP, THALES	**Reviewers**	PMB

This document is issued in the frame and for the purpose of SECUR-ED project. This project has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 261605.

History

NB: a **status** is associated to each step of the document lifecycle:

- **Draft**: this version is under development by one or several partner(s);
- **Under review:** this version has been sent for review;
- **Issued**: this version of the document has been submitted to EC.

Version	Status	Date	Author	Main Changes
1.0	Draft	16.05.2014	ASTS	Initial draft
1.1	Draft	31.07.2014	THALES	Comments
1.2	Draft	01.08.2014	ASTS	Adjustments and extensions
1.3	Under review	08.09.2014	ASTS	Extensions
1.4	Under review	29.09.2014	ASTS	Included comments from RATP, BT and MTRS4
2.0	Issued	30.09.014	THALES	Final version sent to the Commission

TABLE OF CONTENTS

1 Abstract & Purpose

1.1 Abstract

This document considers and consolidates the results of the system solution and/or technologies implemented and experienced in the four main demonstrations (Milano, Paris, Madrid and Berlin), focusing on:

- the level of compliance with the stated goals for each demonstration scenario;
- the level of fulfillment of global security needs;
- the investigated and implemented alternatives in terms of technical solution;
- how the solutions could be open to be adapted to face new threat scenario;
- how they can be efficiently used to enhance security in other conditions (non-intentional event, incivilities and small offences, criminality, ...).

The collection of demonstrations served to illustrate the security needs of Public Transport Operators (PTOs) across Europe and the maturity of modern technologies and design that together support harmonized migration from legacy systems.

This document assumes that the reader is familiar with the SECUR-ED project, its objectives and the respective scenarios of the four flagship demonstrations.

1.2 Purpose of the document

The purpose of this document is to formalize the functional results of the four main demonstrations (Madrid, Paris, Milano and Berlin) in a systematic way. In accordance with the “Guideline for Results Consolidation” document (D46.1), a collection of information, constraints and results were gathered.

Following the proposed approach of considering each demo scenario as a set of field experiments, each analysed in its own right, we have extracted and put together information in order to:

- arrive at practical conclusions as to the achievement of the specific goals;
- extract conclusions relevant to other scenarios/situations/operations.

1.3 Structure of the document

The document is structured in sections as follows:

- Abstract & Purpose (current section);
- References;
- Rationale & methodology;
- Functional Results;
- Conclusions.

2 References

2.1 List of acronyms

COTS	Commercial Off-The-Shelf
EC	European Commission
EU	European Union
ICT	Information & Communication Technologies
IPR	Intellectual Property Rights
ISO	International Standards Organisation
LAN	Local Area Network
LRT	Light Rail Transit
LRV	Light Rail Vehicle
OCC	Operations Control Centre
OEVD	On board Empty Vehicle Detection
PA	Public Address (System)
PIS	Passenger Information System
PSIM	Physical Security Information Management
PTA	Public Transport Authority, sometimes referred as *Public Transport Organizing Authority*
PTO	Public Transport Operator
QA	Quality Assurance
QC	Quality Control
R&D	Research and Development
RFID	Radio Frequency Identification
RTD	Research & Technological Development
SECUR-ED	Secured Urban Transportation – European Demonstration
SOA	Service-Oriented Architecture
SoA	State of the Art
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WP	Work Package

2.2 Referenced documents

The following documents are referenced:

R[1] COUNTERACT / PT5 - Public transport security planning - organisation, countermeasures & operations guidance. Available at http://www.uitp.org/knowledge/projects-details.cfm?id=433

R[2] SECUR-ED D21.1 - Public Transport Security Terms & Definitions

R[3] SECUR-ED D21.3 - Overall Approach to Security Management and Emergency Preparedness

R[4] SECUR-ED D51.2 - Experimentation Building Manual

R[5] Transit agency security and emergency management protective measures, Federal Transit Administration (FTA), November 2006

R[6] Transit Security Design Considerations, Federal Transit Administration (FTA), November 2004

R[7] Technical Recommended Practice for the Selection of Cameras, Digital Recording Systems, Digital High-Speed Networks and Train-lines for Use in New Transit-Related CCTV Systems, APTA Technical Standards document, August 2008

R[8] MODSafe Modular Urban Transport Safety and Security Analysis, Deliverable No. D 9.1 - Hazard scenarios related to security aspects

R[9] Institute for Security & Open Methodologies www.isecom.org

R[10] Physical Security Information Management www.psimtrends.com

R[11] An introduction to video content analysis industry guide, British Security Industry Association, June 2009

R[12] Railway industry website www.railway-technology.com

R[13] ISO 31000, Risk Management Standard

R[14] SECUR-ED D4x.1.- Detailed scenarios for demos Madrid, Paris, Milan, Berlin

R[15] SECUR-ED D4x.2.- Functional specifications for demos Madrid, Paris, Milan, Berlin

R[16] SECUR-ED D46.1.- Guideline for Results Consolidation

R[17] SECUR-ED D4x.5.- Consolidated Results for demos Madrid, Paris, Milan, Berlin

R[18] SECUR-ED D23.4.- Report on Lessons Learned

3 Rationale & methodology

Following the "Guideline for Results Consolidation" (D46.1), the present document is the outcome of the Task 46.2 and it extracts, collects and documents the functionalities, which were intended to be covered by each SECUR-ED flagship demonstration.

The flagship demonstrations have allowed for an evaluation of a large set of security functions across a broad band of realistic scenarios. As a result, different opinions/perspectives related to the same functionality were drawn based on its specific use case. Hence, we report on the specific evaluations of each operator and system integrator according to the specific threats experienced.

The scope of the document is focusing on evaluation of the functionalities in accordance with the indicators suggested in R[16]:

- level of compliance with the stated goals for each demonstration scenario; compliance with the high-level objectives;
- level of fulfilment of the security needs/requirements;
- potential alternatives in terms of technical solutions;
- openness and adaptability to new threat scenarios;
- usability/applicability in other conditions/requirements, i.e. non-intentional events, vandalism small offences, criminality, etc.

Furthermore, the contribution of these functionalities to the achievement of the overall goal of the demo is highlighted in term of criticality as following:

- *Critical*: overall goal cannot be achieved without the particular functionality;
- *Important*: overall goal can be achieved either by reduced functionalities or through alternatives means;
- *Marginal*: overall goal is only marginally affected.

The methodology is based on the collection of the Functional Template compiled by operators and integrators of each demo in order to acknowledge impressions, difficulties, benefits, experiences and teachings in order to synthesize, formalize and infer the information related to each bullet above.

4 Functional Results

4.1 Introduction

One of the key project challenges concerned the identification of solutions that would address the security needs of not only large urban public transportation networks but also those of mid-sized European cities; and in conjunction, respecting fundamental social, legal, and ethical aspects at European-wide and local levels. In order to reach this goal, multiple threats of different nature such as terrorism and urban crimes have been considered; including ways to manage and respond to emergency situations. Starting from threats and potential crisis situations, the security needs of mass transportation have been distinguished and addressed with an integrated and consistent mix of technologies, services and best practices.

The aim of the project was to validate the maturity of modern technologies and prove its readiness by integrating them into existing systems and demonstrating them in operations. In conjunction, lessons learnt; best practices; and guidelines in the design and implementation of security solutions have been documented. This also includes elaboration on the kinds of considerations appropriate when considering solutions to the different environments of each transportation system (i.e.: country, size, threats, number of passengers and future improvements/investments). This document gathers the evaluations of the operators for each experimented capacity, highlighting its own importance in fulfilling the security aims of each particular scenario and the applicability of solutions under its applied context. In particular, this document aims at highlighting sets of functional requirements that proved invaluable in serving the security needs of the heterogeneous environments of European Public Transport Operators. Furthermore, the requirements and constraints of some of the proposed innovative technologies that would fulfil the security needs of the transportation systems are highlighted. Accordingly, the document describes the functional requirements necessary to adapt security technologies to the transportation environments.

4.2 A glance at the four main demos

The objective of the demos was to integrate adequate security capacities (technical and operational) in realistic scenarios with minimal impacts on the existing urban transport system (service performances, freedom of movement, privacy, etc.), while taking into account the specific environment (legacies). The main demos were performed in Milan, Paris, Madrid and Berlin.

The *Milan* demonstration addressed the following four scenarios:

- Scenario 1 concerned the identification and tracking of persons presenting a suspicious behaviour within the network of public transport managed and owned by different PTOs;
- Scenario 2 was related to the protection of a train in a stabling area and depot yard*;*
- Scenario 3 dealt with the reaction to an event in case of emergency and the subsequent management of the crisis;

- Scenario 4 demonstrated the possible visualization and coordination of local procedures of different stakeholders through the implementation of a local System of Systems in the Milan Area.

The *Paris* demonstration consisted of five scenarios:

- Scenario 1 concerned the protection of critical network and IT systems against cyberattack;
- Scenario 2 focused on the protection of an interchange node against an attack using toxic materials;
- Scenario 3 was related to the protection of an interchange node against an attack using radioactive materials;
- Scenario 4 proved cross function operation of CCTV and use of video analytics applications;
- Scenario 5 involved the protection of an interchange from an attack using explosives.

The *Madrid* demonstration also consisted of five scenarios:

- Scenario 1 concerned the creation of new procedures in order to integrate them inside the Madrid demo;
- Scenario 2 tested the management tools;
- Scenario 3 regarded how the incident management system and a geographical information system allowed interoperability among different stakeholders;
- Scenario 4 added an intermodal CCTV to scenario 3 in order to check the efficiency of decision making procedures;
- Scenario 5 checked the efficiency of communications between Control Centres and vehicles in case of incident.

The *Berlin* demonstration answered to multiple and different threats such as criminal activities (pickpocketing, vandalism, fare evasion and public disorder), anonymous bomb threats, suspicious objects, assault with a cold weapon (any weapon that does not involve shooting or explosions), dispersion of toxic material, large events control. Differently to the other demos the approach was the realization of a training programme in order to cover the above threats. From this perspective, six scenarios were run:

- Scenario 1 focused on the implementation of standard and emergency operating procedures (SOP), field level security plans and a decision making model for threat, emergency and crisis situations;
- Scenario 2 involved the execution of security awareness training programmes for front-line employees, passengers and top management;
- Scenario 3 concerned the execution of training programmes for security employees;
- Scenario 4 regarded the execution of training programmes for operators in control centres;
- Scenario 5 related to the execution of training programmes for security managers;
- Scenario 6 affected the execution of emergency and crisis preparedness training programmes.

To sum up the SECUR-ED approach, the Table 1 outlines the main adopted security solutions or functionalities related to the specific security needs. The latter have been fulfilled performing the attack scenarios in the four main demos as described above by means of an integrated approach SOA-based. In particular, the demos have demonstrated the feasibility of the chosen approach, which allowed the coexistence of new and legacy technologies and with a minor implementing effort. Finally, the Table 2 outlines the security needs taken account in each demo while the Table 3 shows the functionalities in each main demo.

Functionalities / Security needs	Telecommunication systems	CCTV systems	Video Analysis	CBRNE systems	Cyber technology	RFID	Localization technology	Emergency procedures	Integrated Information Management Tools	Operator training & simulation
Intrusion detection	x	x	x				x	x	x	
Dangerous material detection			(x)	x				x	x	
Tracking & Facial Recognition	x	x	x			x	x	x	x	
Cyber Attack detection & resilience	x				x				x	
Identification of potential threats		x	x				x		x	x
Early reaction to crisis	x	x	x	x			x	x	x	x
Incident Management	x	x					x	x	x	x

Table 1-Security needs and related functions implemented

Demo / Security needs	Madrid (Ma)	Milan (Mi)	Paris (P)	Berlin (B)
Intrusion detection		X	X	
Dangerous material detection		X	X	
Tracking & Facial Recognition		X	X	
Cyber Attack detection			X	
Identification of potential threats			X	X
Early reaction to crisis	X	X		X
Incident Management	X		X	X

Table 2- Security needs fulfilled in main demos

Demo / Functionalities	Madrid (Ma)	Milan (MI)	Paris (P)	Berlin (B)
Telecommunications systems	X	X	X	
CCTV systems	X	X	X	X
Video Analysis		X	X	
CBRNE systems		X	X	
Cyber protection technology			X	
RFID		X		
Localization Technology	X		X	X
Emergency procedures	X	X	X	X
Integrated Information Management Tools	X	X	X	X
Operator training & simulation		X		X

Table 3-Functionalities in main demos

4.3 Analysis of SECUR-ED functionalities

This section synthesizes the functional results for each functionality according to indicators identified in R[16] and reported in section 3. The outcomes are produced in term of:

- criticality;
- level of compliance;
- fulfilment of the security need with respect to the employed functionality;
- openness and adaptability of the functionalities estimated also on basis of the experience of satellite demos;
- potential alternatives.

4.3.1 Integrated Information Management Tools

As can be determined from the above tables integrated information management tools have been the heart of demos. The demos have demonstrated their strategic role for properly responding to any kind of emergency and to be essential to respond and deal with the wide range of potential security risks. In fact, integration of all identification systems allows the immediate notification of all incidents and greatly increases the preparedness to respond to real security threats with the appropriate resources. Also, by means of SOA approach and standard protocols, the openness and adaptability to new scenarios and environments has been completely achieved.

As a result, the following tables point out the contribution for each subcategory of this functionality in term of criticality, level of compliance and fulfilment of the security need with respect to the employed functionality.

Integrated Information Management tool	Critical	Important	Marginal
Supervision Server(s)	Ma-Mi-P		
Orchestration Engine	Ma	P	
Post-event Analysis		P	Ma
Passenger Information		Ma	
Decision Support Systems		P	
Operator Workstation	Ma		

Table 4-Criticality of Integrated Information Management Tools

Integrated Information Management tool	Very High	High	Medium	Low	Very Low
Supervision Server(s)	Mi - P				
Orchestration Engine	Ma - P				
Post-event Analysis	P				
Passenger Information		Ma			
Decision Support Systems		P			
Operator Workstation	Ma				

Table 5-Level of compliance of Integrated Information Management Tools

Integrated Information Management tool	Yes	No	Not completely
Supervision Server(s)	Ma-Mi-P		
Orchestration Engine	Ma-P		
Post-event Analysis	P		
Passenger Information	Ma		
Decision Support Systems	P		
Operator Workstation	Ma		

Table 6-Fulfilment of security needs of Integrated Information Management Tools

Potential Alternatives: NA

4.3.2 Telecommunication systems

The demos have proved that the tested telecommunications systems are an advantageous solution as an enabler to many modern security applications; by providing the means to wireless communicate video, voice, and data between vehicles and operation control centres. For example in the Milan demonstration it allowed the use of the OEVD (On-board Empty Vehicle Detection) system that detected passengers and objects left on-board based on intelligent video image processing technology.

Other technical alternatives of interest but excluded from studies include NFC and Bluetooth.

As before, we summarize in the following tables some relevant aspects.

Telecommunication systems	Critical	Important	Marginal
Communication between vehicles and wayside		Ma-Mi-P	
Multimedia transmission between field and wayside security staff		P	
Info Transmission by Smartphone		Mi-P	

Table 7-Criticality of Telecommunication systems

Telecommunication systems	Very High	High	Medium	Low	Very Low
Communication between vehicles and wayside		Ma-Mi-P			
Multimedia transmission between field and wayside security staff		P			
Info Transmission by Smartphone		Mi-P			

Table 8-Level of compliance of Telecommunication systems

Telecommunication systems	Yes	No	Not completely
Communication between vehicles and wayside	Mi-P		Ma
Multimedia transmission between field and wayside security staff	P		
Info Transmission by Smartphone	Mi-P		

Table 9-Fulfilment of security needs of Telecommunication systems

4.3.3 CCTV Systems &Video Analysis

CCTV systems also play an important role and are very useful in both indoor and outdoor applications. It was validated that, to ensure the effectiveness and reliability for the majority of video analytics solutions, it is of significant advantage and importance to select CCTV cameras that do not only operate under the environmental conditions that they may be exposed to year-round (e.g. temperature, lighting conditions, etc.), but also having the cameras professionally installed at locations specifically optimised for the intended functionalities sought by the applied video analytics.

None of the video analytics solutions demonstrated were intended for replacing human intervention. Rather, the video analytics solutions proved to effectively support the security operators; complementing their existing duties by better exploiting the functionalities and uses offered by CCTV cameras. In general, video analytics are helping re-shift the use of CCTV cameras for greater real-time application versus passive forensic use. Furthermore, they have proven to provide substantial security advantage for security operators by enhancing their vigilance to potential hazardous situations.

Examples include the demonstrated intrusion detection solutions which proved to be more effective in detecting intrusion than security operators, especially considering that security operators typically have an overwhelming number of monitors to observe.

The On-board Empty Vehicle Detection system also proved to be versatile in its application being extendable to detect not only passengers but also abandoned luggage.

The suspect tracking video analytic was also desired by the operators to support them in more easily tracking individuals across their network of CCTV cameras; especially when combined with geo-location of the suspect on maps.

Another innovative solution included the active facial recognition installed in a bus of RATP in Paris. During the demo the system correctly recognized the suspect and generated an alarm to the supervision system.

The tables below highlight findings of each Operator (Ma = Madrid, Mi = Milan, P = Paris, B = Berlin) with respect to each set of capacities.

CCTV Systems & Video Analysis	Critical	Important	Marginal
Basic CCTV services	Ma-Mi-P		
Intrusion / Presence detection	Mi		
Tracking person	Ma-Mi-P		
Crowd detection		Mi	
Massive fall detection	P		
Facial recognition		P	
On board Empty Vehicle Detection	Mi		

Table 10-Criticality of CCTV Systems & Video Analysis

CCTV Systems & Video Analysis	Very High	High	Medium	Low	Very Low
Basic CCTV services	Ma-Mi-P				
Intrusion / Presence detection	Mi				
Tracking person		Ma-Mi-P			
Crowd detection		Mi			
Massive fall detection		P			
Facial recognition		P			
On board Empty Vehicle Detection		Mi			

Table 11-Level of compliance of CCTV Systems & Video Analysis

CCTV Systems & Video Analysis	Yes	No	Not completely
Basic CCTV services	Ma-Mi-P		
Intrusion / Presence detection	Mi		
Tracking person	Ma-Mi-P		
Crowd detection	Mi		
Massive fall detection	P		
Facial recognition	P		
On board Empty Vehicle Detection	Mi		

Table 12-Fulfilment of security needs of CCTV Systems & Video Analysis

4.3.4 CBRNE systems

From experience of demos, we can confirm that the CBRNE systems are a good security solution for environmental monitoring and train scanning. As expected, thanks also to the adopted integration strategy, their alerts were sent to staff and they were able to apply the relevant procedure. For the chemical sensor used in one demo, some problems about the coverage range have been highlighted while the radiological and explosive ones have properly worked for the assigned purpose. Specific tools dedicated to explosive detection, combined with dog patrols, demonstrated the ability to analyse what dangerous material the passengers carry and to generate an alarm for the staff to apply the relevant procedure. As previously, we report the tables in according to illustrated indicators.

CBRNE systems	Critical	Important	Marginal
Chemical material detection		Mi-P	
Radiological material detection		Mi-P	
Explosive material detection		P	

Table 13-Criticality of CBRNE systems

CBRNE systems	Very High	High	Medium	Low	Very Low
Chemical material detection		P	Mi		
Radiological material detection		Mi-P			
Explosive material detection		P			

Table 14-Level of compliance of CBRNE systems

CBRNE systems	Yes	No	Not completely
Chemical material detection	P		Mi
Radiological material detection	Mi-P		
Explosive material detection	P		

Table 15-Fulfilment of security needs of CBRNE systems

The CBRNE sensors are very specific technologies for particular threats so there are no potential alternatives so far and, although applicable and adaptable in different contexts, do not react to threats different from those considered by scenarios.

4.3.5 Cyber technology

For this capacity, which includes the associated procedures, the main goal was to make visible to the security operators how an extensive use of ICT in the systems introduces a new potential vulnerability. Cyber technology does not prevent from putting in place the appropriate physical protection of sensitive premises. The following tables summarize some results.

Cyber technology	Critical	Important	Marginal
Cyber protection		P	

Table 16- Criticality of Cyber technology

Cyber technology	Very High	High	Medium	Low	Very Low
Cyber technology		P			

Table 17- Level of compliance of Cyber technology

Cyber technology	Yes	No	Not completely
Cyber technology	P		

Table 18- Fulfilment of security needs of Cyber technology

There is no real alternative other than coming back to electromechanical systems without any ICT. A possible way is to change the approach to systems design introducing the cyber security from the first phases of project.

The cyber technologies have been integrated in the satellite demo of Lisbon proving its applicability to a new threat scenario.

4.3.6 RFID

The RFID technology has been a good security solution. However, some issues about the detection distance was pointed out, for this reason in each critical point has been installed a double system of antennas, to have more possibilities that the solution worked well.

RFID	Critical	Important	Marginal
RFID ticket tracking		Mi	

Table 19-Criticality of RFID

RFID	Very High	High	Medium	Low	Very Low
RFID ticket tracking		Mi			

Table 20-Level of compliance of RFID

RFID	Yes	No	Not completely
RFID ticket tracking			Mi

Table 21-Fulfilment of security needs of RFID

Other technical alternatives could be solutions based on NFC, Bluetooth and Wi-Fi.

4.3.7 Localization Technology

This technology brought a significant improvement in the security of public transport system achieving some advantages like avoiding risks situations for vehicles close to the hotspot thanks to the location of all vehicles inside the influence area, or optimising the restoration of activities. So, it noticeably allow enhancements of the crisis management (e.g. for sending a rescue team in emergency events in order to save lives). Considering this, the functionality is able to react to several threats that require emergency services intervention. The tables below summarize the evaluation of operator.

Localization Technology	Critical	Important	Marginal
Geographical Information System	Ma		

Table 22-Criticality of Localization Technology

Localization Technology	Very High	High	Medium	Low	Very Low
Geographical Information System	Ma				

Table 23- Level of compliance of Localization Technology

Localization Technology	Yes	No	Not completely
Geographical Information System	Ma		

Table 24-Fulfilment of security needs of Localization Technology

Potential alternatives: NA

4.3.8 Operator Training, Emergency procedures & Simulation

The simulation capacity has been used in two different contexts proving its own flexibility: in Milan for the evacuation modelling and in Berlin for simulating the training of operators of a CCTV system in the security control room.

The Milan feedback about the demonstration of the evacuation modelling system was very good and it has completely answered the security need of the operator. The results have been compared to a real evacuation of the considered station, performed with volunteers. As expected, the real simulation of the evacuation was not optimal - slower than in a real risky event - because “passengers” were aware of the simulated nature of the event. Thereby, this simulation capacity is a very good alternative to test additional configurations of evacuations and avoids various low-effective drills. It can simulate different situations, events, in various environments such as stations, depots, lines, etc. It could even be used to test infrastructures before their construction. The strength of this capacity was that the simulator is totally independent from the operational activities and can be run without interacting with the normal operations.

Regarding the preparedness of staff, the Berlin experience has highlighted that the implementation of emulation capacities still faces some challenges, such as the transfer of the user interface of the simulator software to the native language of the operators. In addition, the software tools used daily by the operators and the simulation software should be the same or at least similar, e.g. with respect to functionalities, interaction patterns and usability. Other interesting features are available, such as the immediate playback of CCTV videos during operations, even if not applicable in some European countries due to rules & regulations. Therefore, even such a straightforward approach to simulate critical situations still needs some transfer effort, which either has to be done by the trainee, by the trainer, or already during the preparation of the simulation environment and the simulation content.

More generally, as far as training demos were concerned, the results are nearly the same for each of them. All trainings were informative, and generated much interest among the participants. As a consequence, the employees were able to learn new methods to enhance identification of relevant hazardous situations. Finally, they understood and learned best practices to handle routine and emergency situations more efficiently (e.g. what to look for, who to inform, what to do and so on) by means of a training platform based on a PSIM system.

The following tables sum up the gathered evaluations.

Operator Training, Simulation & Emergency procedures	Critical	Important	Marginal
Security training course for front-line employees		B	
Security awareness course for passengers		B	
Security CBT for recurrent awareness training of front line employees		B	
Security training course for security agents		B	

Security refresher CBT course for security agents		B	
Security training course for operators in security command and control centres		B	
Simulator training for operators of CCTV system in the security control room		B	
Security training course for security managers		B	
Emergency and Crisis Preparedness Training Programme	B		
Evacuation modelling	Mi		
Incident Response Plan		Ma	
Organisational & operational procedures and plans	Ma-B		

Table 25- Criticality of Operator Training, Simulation & Emergency procedures

Operator Training, Simulation & Emergency procedures	Very High	High	Medium	Low	Very Low
Security training course for front-line employees			B		
Security awareness course for passengers			B		
Security CBT for recurrent awareness training of front line employees			B		
Security training course for security agents	B				
Security refresher CBT course for security agents			B		
Security training course for operators in security command and control centres		B			
Simulator training for operators of CCTV system in the security control room	B				
Security training course for security managers		B			
Emergency and Crisis Preparedness Training Programme	B				
Evacuation modelling	Mi				
Incident Response Plan	Ma				
Organisational & operational procedures and plans	Ma				

Table 26- Level of compliance of Operator Training, Simulation & Emergency procedures

Operator Training, Simulation & Emergency procedures	Yes	No	Not completely
Security training course for front-line employees	B		
Security awareness course for passengers		B	
Security CBT for recurrent awareness training of front line employees		B	
Security training course for security agents	B		
Security refresher CBT course for security agents		B	
Security training course for operators in security command and control centres	B		
Simulator training for operators of CCTV system in the security control room	B		
Security training course for security managers	B		
Emergency and Crisis Preparedness Training Programme	B		
Evacuation modelling	Mi		
Incident Response Plan	Ma		
Organisational & operational procedures and plans	Ma		

Table 27-Fulfilment of security needs of Operator Training, Simulation & Emergency procedures

4.3.9 Other Functionalities

Here some evaluations about other functionalities used during demos.

Other	Critical	Important	Marginal
QR Code			Mi
Ticketing System		Mi	

Table 28- Criticality of other functionalities

Other	Very High	High	Medium	Low	Very Low
QR Code		Mi			
Ticketing System		Mi			

Table 29- Level of compliance of other functionalities

Other	Yes	No	Not completely
QR Code	Mi		
Ticketing System	Mi		

Table 30- Fulfilment of security needs of other functionalities

The use of other functionalities has confirmed the openness of the modular system to take advantage of additional technologies. This has demonstrated how all kind of technologies can contribute to increase the security, if opportunely integrated.

5 Conclusions

This document serves to provide a summary of the SECUR-ED flagship demonstration results from a functional point of view.

The flagship (and satellite) demonstrations have validated the maturities of modern technologies and the realm of possibilities in adapting them to existing operating environments to directly address the security challenges faced in urban transportation. In addition, SECUR-ED experience confirms that to improve the exploitation of the technologies, it is essential to have a strong cooperation between operators, researchers and technicians to ensure a holistic understanding of mutual requirements and propositions that are of value.

Some hurdles in mainstreaming a number of security innovations to the transportation industry include aspects that may pertain to ethical, legal, social, economic, and culture. For example, the use of facial recognition algorithms is ethically controversial and faces problems of legal authorizations.

One important mentality SECUR-ED took was to avoid reinventing the wheel. This approach was exemplified through the encouragement of deriving solutions with commercial-off-the-shelf products where possible and compliance to Service Oriented Architecture which contributed a level of modularity to the solutions derived.

To further support the usability of derived solutions, one design element encouraged in the derivation of the capacities was to have them as easy to adapt and deploy as possible to lessen (if not eliminate) any requirement of needing further professional support beyond what would typically be available to operators in - house.

A Security Management System is the heart of security systems and its functionalities have been shared and consolidated in all demos. Functional characteristics of this system are dictated by end users. All operators demand simple & user-friendly software that has an intuitive and easy to use interface. Operationally, the central control system monitors and manages events detected by new and legacy systems with real time interactions and procedures driven by decision support system. The most important conclusion is that functionalities can be adapted and managed with a hierarchy of operations. This was pointed out to be a critical element to support operators' crisis management procedures and also to allow concurrent system supervision and maintenance without interruption of services. Other critical functionalities for Security Management Systems include interactive management of alarms, and automatic display of alarms in real time.

Another important functionality valued by the operators from the demonstrations was the availability of additional information pertaining to the alarms received. This included: event description, priority, timestamp, status, and source; which enabled them to more effectively manage the lifecycle for a given alarm. Moreover some operators have preferences over user interfaces that have colour-coded information, sound, and pictures/visuals of the state of devices; including its geo-location. Operational procedures (work flow) management is a strategic functionality for Security Management Systems of utmost importance in transportation systems. It is necessary to associate each alarm with a standard operating procedure. The procedure helps the operator to manage the situation and share information with other stakeholders until responsibilities are passed on to other authorities to preserve the safety and security of a city.

Finally it is worth noting that the overall SECUR-ED future-proof conclusions and recommendations are to be found in the D0.1.11 “SECUR-ED Final Report” and associated White Paper.

- End of document -