

SECONOMICS

D3.3 - Urban public transport requirements final version

R. Munné (Atos), M. Pellot (TMB), Ricardo Ortega (TMB), Daniel Villegas (TMB), Martina de Gramatica (UNITN), Woohyun Shim (UNITN), E.Chiarani (UNITN), J.Williams (UNIABDN), P.Guasti (ISAS CR), Z.Mansfeldova (ISAS CR)

Pending of approval from the Research Executive Agency - EC

Document Number	D3.3
Document Title	Urban public transport requirements final version
Version	0.20
Status	Final
Work Package	WP 3
Deliverable Type	Report
Contractual Date of Delivery	31.01.2013
Actual Date of Delivery	20.12.2013
Responsible Unit	Atos
Contributors	UNITN, TMB, ISAS CR
Keyword List	urban transport, security, use case, requirements
Dissemination level	PU

SECONOMICS Consortium

SECONOMICS “Socio-Economics meets Security” (Contract No. 285223) is a Collaborative project) within the 7th Framework Programme, theme SEC-2011.6.4-1 SEC-2011.7.5-2 ICT. The consortium members are:

1	 UNIVERSITÀ DEGLI STUDI DI TRENTO	Università Degli Studi di Trento (UNITN) 38100 Trento, Italy www.unitn.it	Project Manager: prof. Fabio MASSACCI Fabio.Massacci@unitn.it
2	 DEEPBLUE	DEEP BLUE Srl (DBL) 00193 Roma, Italy www.dblue.it	Contact: Alessandra TEDESCHI Alessandra.tedeschi@dblue.it
3	 Fraunhofer ISST	Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., Hansastr. 27c, 80686 Munich, Germany http://www.fraunhofer.de/	Contact: Prof. Jan Jürjens jan.juerjens@isst.fraunhofer.de
4	 Universidad Rey Juan Carlos	UNIVERSIDAD REY JUAN CARLOS, Calle TulipanS/N, 28933, Mostoles (Madrid), Spain	Contact: Prof. David Rios Insua david.rios@urjc.es
5	 UNIVERSITY OF ABERDEEN	THE UNIVERSITY COURT OF THE UNIVERSITY OF ABERDEEN, a Scottish charity (No. SC013683) whose principal administrative office is at King's College Regent Walk, AB24 3FX, Aberdeen, United Kingdom http://www.abdn.ac.uk/	Contact: Prof. Julian Williams julian.williams@abdn.ac.uk
6	 TMB Transports Metropolitans de Barcelona	FERROCARRIL METROPOLITA DE BARCELONA SA, Carrer 60 Zona Franca, 21-23, 08040, Barcelona, Spain http://www.tmb.cat/ca/home	Contact: Michael Pellot mpellot@tmb.cat
7	 Atos	ATOS ORIGIN SOCIEDAD ANONIMA ESPANOLA, Calle Albarracin, 25, 28037, Madrid, Spain http://es.atos.net/es-es/	Contact: Silvia Castellvi Catala silvia.castellvi@atosresearch.eu
8	 SECURENOK	SECURE-NOK AS, Professor Olav Hanssensvei, 7A, 4021, Stavanger, Norway Postadress: P.O. Box 8034, 4068, Stavanger, Norway http://www.securenok.com/	Contact: Siv Houmb sivhoumb@securenok.com
9	 SOU Institute of Sociology AS CR	INSTITUTE OF SOCIOLOGY OF THE ACADEMY OF SCIENCES OF THE CZECH REPUBLIC PUBLIC RESEARCH INSTITUTION, Jilská 1, 11000, Praha 1, Czech Republic http://www.soc.cas.cz/	Contact: Dr Zdenka Mansfeldová zdenka.mansfeldova@soc.cas.cz
10	 nationalgrid THE POWER OF ACTION	NATIONAL GRID ELECTRICITY TRANSMISSION PLC, The Strand, 1-3, WC2N 5EH, London, United Kingdom	Contact: Dr Ruprai Raminder Raminder.Ruprai@uk.ngrid.com
11	 ANADOLU ÜNİVERSİTESİ	ANADOLU UNIVERSITY, SCHOOL OF CIVIL AVIATION İki Eylül Kampusu, 26470, Eskisehir, Turkey	Contact: Nalan Ergun nergun@anadolu.edu.tr

Document change record

Version	Date	Status	Author (Unit)	Description
0.1	30/10/2012	Draft	R. Munné (Atos)	ToC
0.2	15/11/2012	Draft	R. Munné (Atos)	Adapted ToC to common headings for D1.3, D2.3, D3.3
0.3	19/11/2012	Draft	R.Munné (Atos)	Addition of contents Section 3
0.4	27/11/2012	Draft	R. Ortega (TMB), D. Villegas (TMB), M. Pellot (TMB)	Addition of contents Sections 2 & 3
0.5	06/12/2012	Draft	R. Ortega (TMB), D. Villegas (TMB), M. Pellot (TMB), R.Munné (Atos) , W. Shim (UNITN), M. de Gramatica (UNITN)	Addition of contents Sections 2, 3, 4 & 5, including questionnaire that follows some suggestions made by UNITN
0.6.	13/12/2012	Draft	E.Chiarani (UNITN)	First Quality Check completed. Revision requested.
0.7.	28/12/2012	Draft	P.Guasti, Z.Mansfeldova (ISAS CR)	Scientific Review
0.8	02/01/2013	Draft	R.Munné (Atos)	Revision based on 1st quality check
0.9	10/01/2013	Draft	R.Munné (Atos)	Address comments from the internal scientific review
0.10	17/01/2013	Draft	R. Ortega (TMB), D. Villegas (TMB), M. Pellot (TMB), R.Munné (Atos)	Address comments from the internal scientific review. Revision of contents
0.11	28/01/2013	Draft	R. Ortega (TMB), D. Villegas (TMB), W. Shim (UNITN)	Additions to sections 2, 4 & 5
0.12	01/02/2013	Draft	R. Ortega (TMB), D. Villegas (TMB), M. Pellot (TMB), R.Munné (Atos)	Completion of sections 2 & 4. Additions to section 5.1
0.13	13/02/2013	Draft	R. Ortega (TMB), D. Villegas (TMB), M. Pellot (TMB), R.Munné (Atos)	Completion of scenarios in section 4. Review of Executive Summary
0.14	06/03/2013	Draft	R. Ortega (TMB), D. Villegas (TMB), M. Pellot (TMB), R.Munné (Atos)	Completion of 4.1.1, 4.1.2, 4.2 and final revision
0.15	29/03/2013	Draft	E.Chiarani (UNITN), W. Shim (UNITN), M. Pellot (TMB), R.Munné (Atos)	Second Quality Check and Scientific review; some remarks provided and some improvements requested
0.16	24/04/2013	Draft	E.Chiarani (UNITN), W. Shim (UNITN), M. Pellot (TMB), R. Ortega (TMB), R.Munné (Atos)	UNITN quality check (E. Chiarani, some minor remarks) and scientific review (W. Shim, comments provided)



0.17	17/05/2013	Final	E.Chiarani (UNITN), W. Shim (UNITN), J.Williams (UNIABDN), R.Munné (Atos)	UNITN quality check (E. Chiarani, and scientific review (UNITN - W. Shim, UNIABDN - J.Williams). Last requested changes completed for final version
0.18	30/11/2013	Review changes	R. Ortega (TMB), (TMB), M. Pelot (TMB), Zdenka Mansfeldová (ISAS CR), Petra Guasti (ISAS CR), R.Munné (Atos)	Added changes requested after review
0.19	13/12/2013	Review changes	R.Munné (Atos)	Changes requested after scientific review with Julian Williams. English proof-reading
0.20	20/12/2013	Final	R.Munné (Atos)	Final production of report after receiving ok to changes



INDEX

D3.3 - Urban public transport requirements final version.....	1
SECONOMICS Consortium.....	2
Document change record	3
INDEX 5	
Executive summary	7
1. Introduction & Objectives.....	8
1.1 Scope of report	8
1.2 Report Objectives and Results.....	8
2. Further Background to urban transport security	9
2.1 Urban transport security description	9
2.1.1 Focus on security scenarios	9
2.1.2 Detailed description of threats and countermeasures	10
2.1.3 Security objectives of TMB.....	15
2.1.4 Security measures of TMB	18
2.2 Risk prevention framework at TMB	25
2.3 Regulatory framework for underground urban transport	26
2.4 Description of Xarxa4	27
2.4.1 Resource distribution in Xarxa4	27
2.4.2 Distribution of incidents in Xarxa4.....	29
3. Stakeholders & Engagement Plan	30
4. Urban transport scenarios based on current threats	34
4.1 Description of scenarios	34
4.2 Key validation indicators for current threats.....	53
4.3 Effectiveness of security measures	55
5. Urban transport scenarios based on emerging threats	59
5.1 Description of scenarios	60
5.2 Key validation indicators for emerging threats	63
6. Security framework definition for urban public transport.....	64
6.1 Security framework requirements	64
6.2 Stakeholders perspective for a new security framework in the urban public transport ...	65
7. Research questions	67
REFERENCES.....	70
8. ANNEX 1. Xarxa 4 in the context of the Barcelona metro network.....	72



9.	ANNEX 2. Internal validation.....	74
10.	ANNEX 3. Glossary	100
11.	ANNEX 4. Detailed information on security incidents and resources	103

Executive summary

This report presents the final version of TMB requirements for Urban Transport with respect to Work Package 3 of the SECONOMICS project. It follows on from the work documented in SECONOMICS Deliverable 3.2 titled ‘Urban public transport requirements first version’.

This report presents the requirements for Work Package 3 which focuses on understanding and assessing the security environment, that in the case of a public transport, the passengers’ perception of security has an important precedence. The main part of the report develops the security measures used in the TMB metro network, the resources used to implement such measures as well as the risk prevention framework and the regulatory framework in force at TMB. This frame is, to a great extent, the same in force for other Transport Operators in the European Union.

The security scenarios of Work Package 3 have been constructed to cover the widest range of security incidents, existing and emerging, not only at local level, but also those affecting most on European urban transport operators. The effectiveness of the security measures is provided as a complement of the information provided in the scenarios. It is specifically addressed the identification and management of new and emerging threats and their relation with the described scenarios.

The perspective of stakeholders regarding the security is provided from inputs collected during the validation and dissemination activities conducted as part of the project tasks.

The security scenarios and discussion on the security dimension that affect the transport user’s security regulatory structures provide a thorough background to progress the building of models that will be relevant to other Public Transport Operators.

1. Introduction & Objectives

1.1 Scope of report

This report is the final version of TMB requirements. It builds upon the work undertaken in the earlier report Deliverable 3.2 (D3.2) titled '*Urban public transport requirements first version*'.

The present report extends the concepts and scenarios defined there. It also develops the external stakeholders' involvement plan, which is very important to engage them for the next phase and to obtain their feedback and validation on the work developed.

Due to the fact that it is a public service used by 1.3 million travellers each working day, 388.98 million travels per year [1], security measures adopted have a great impact in the users, and therefore in the society. For that reason section 6 "Security framework definition for urban public transport" offers a strategic view of the social implications of security in the urban transport.

1.2 Report Objectives and Results

The objectives and results presented in this report are the following:

- Giving further background to the already provided in the first version of the requirements, refining the selected security scenarios, and detailing the socio-economic causes behind them;
- Detailed description of the urban transport scenarios, with the specific threats and countermeasures applied;
- A description of the key validation indicators to detect variations in the security incidents based on the typified security incidents of the scenarios;
- Identification of future and emerging threats based on current crisis environment and new social phenomena;
- Introduction of security framework requirements based in the scenarios analysed.

The report presents a detailed analysis of the security scenarios based on risk and sociological impacts, caused not only by the material and immaterial damages, but also due to the costly prevention measures required due to the complexity, and the variety of stakeholders involved that have influence over an urban transport system like this.

2. Further Background to urban transport security

2.1 Urban transport security description

In this section we will go through and extend and deepen the analysis of the security environment description provided in the first version of requirements, which merited further development. In this section security measures used in TMB metro network are detailed, describing the different types of security measures employed, human, procedural and technical resources. Also resources and incidents distribution in Xarxa4¹ - the portion of the Barcelona Metro network being considered for the scenarios described in this report- with regard to the whole network are detailed. The security objectives for Xarxa4 are also specified as well as the threats and countermeasures applied.

2.1.1 Focus on security scenarios

Since the project is mainly focused on the social impact of the security measures applied by the Public Transport Operator, those incidents that affect, directly or indirectly, the sense of security or objective security have been chosen. These types of security incidents have, as well, a direct impact on customers and / or service.

It should be noted, however, that some security-related phenomena have not been considered in the security scenarios for specific reasons. For example, to fight against terrorism, information, analysis and intelligence tools are required, but they are not available to transport operators like TMB. Such tools for security analysis are within the scope and responsibility of the law enforcement agencies.

TMB works in conjunction with law enforcement agencies to apply preventive and dissuasive operational measures. In this sense, there is a continuous collaboration with those agencies, as the metro facilities are considered an extension of the public space, as it is a means of mass transportation.

Examples of collaboration in the case of TMB are:

- the use of sniffer dogs for the detection of explosives when a suspicious abandoned object is found in the metro facilities (as detailed in section 2.1.4);
- access to CCTV video recordings required by the security forces for police and judicial investigation.

Other preventive actions to be performed against terrorism are largely beyond the scope of the competences of the Transport Operator. The peculiarity of transport itself prevents the application of effective and efficient security measures against such phenomena, as accessibility and massive nature of this type of public transport takes precedence.

In the case of information security threats it is not possible that they can affect the service or passenger's security due to the technical infrastructure in use in the railway environment and specifically at TMB. Service control systems are of exclusive use in the railway sector, which are provided by the manufacturers of such systems. The communication between those systems takes place in private communication lines (not

¹ ANNEX 1. Xarxa 4 in the context of the Barcelona metro network.

connected to the external world), the communication infrastructure is completely of private use by TMB, wires are laid along the same facilities as the tracks, so for this reason it is not considered any threat of this type that could affect the service and therefore the security of the passengers. Of course, other systems related to the management of the company (not the service), like for example, accounting and payroll systems and external websites can be affected by cyber security threats, but this cannot have any impact on service and passenger's security.

Nevertheless, there have been identified other interesting scenarios related to civil disorder, some of them more common in public transport and other new and emerging. These identified scenarios could be applied to a largest number of operators and cities, as those types of incidents are the most common and permanent in the vast majority of Public Transport Operators, either by its prevalence and / or by its impact at economic and social level. Those scenarios are detailed in section 4.1

The security incidents in the identified scenarios have been typified according to behaviour in the following classification following advice by security experts from the UITP²:

- **Uncivic behaviour:** Individual and / or sporadic behaviour not adjusted to socially accepted code of conduct, which causes a state of uneasiness and discomfort in people who witness it.
- **Antisocial behaviour:** Behaviour of an organized nature and / or intentional or recidivist involving violations of criminal or administrative regulations with a clear social disdain.
- **Criminal behaviour:** Behaviour defined in the criminal laws in force.

Each incident can be qualified within one or more of those categories depending of their nature: that determines the way it should be treated.

2.1.2 Detailed description of threats and countermeasures

The previous described classification is based on a cross pattern, considering both the cause that motivates them, and the final outcomes. For that reason, both are appreciated, the purpose (goals) as well as how the action is carried out: whether it is performed by individuals or in an organized or planned way. For this reason such classification is an optimal starting point to set the countermeasures used to deal with each type of incident.

In order to illustrate categories and the corresponding countermeasures for each incident, we use “traveling without transport ticket” as an example, as it covers all three categories:

- **Uncivic behaviour:** Fraud that is done intentionally in order to travel without paying the ticket, offending and disturbing the citizens who pay their ticket.

² International Association of Public Transport

Proportionate and effective countermeasures against this type of incidents are: administrative complaints, deterrence by the occasional presence of security guards or employees in the station hallways, through information and communication campaigns towards the users.

- Antisocial behaviour [2]: Fraud that is performed by a group of people not simply with the intention to travel without paying the ticket, but with the intention to make a particular claim, usually associated with the cost of the tickets. The real purpose of the offenders is to get media coverage of the event, so any provocation or incident occurred can give them the opportunity to increase the consequences and impact of their actions, while justifying its need, its continuation and frequency. Therefore, countermeasures to be applied to this type of incidents cannot be the same as for an Uncivic fraud, as administrative complaints towards this group of users can be counterproductive and inoperative in relation to the number of offenders and the number of security guards available. Therefore, countermeasures to be applied are just to prevent vandalism, with a slight presence of security guards that will act only if some type of crime is committed, not fraud.
- Criminal behaviour (Scam): There are several subtypes associated with this category. On one hand the individual using a tampered transport ticket (modified or counterfeit) purchased outside the authorized points of sale. On the other hand the individual using a tampered transport ticket (modified or counterfeit) that he is not aware of it. Countermeasures move in the field of criminal justice, as it is a manipulation of a commercial document. The point of manufacture and sale of tampered transport tickets falls also in this criminal category that, depending on whether it is with the aim of making profit or protest, must be countered with advanced criminal investigation techniques and / or with awareness campaigns based on the impact of the scam.

Table 1 shows a wide list of different categories used at TMB that can be associated with each type of security events, according to the criteria explained above. Some of those are very generic because they group different concrete issues. Not all of these are included in the scenarios. The specific events included in each scenario are explained in each scenario description.

Table 1. Classification of security events in TMB (source TMB)

Types of security events	Uncivic	Antisocial	Criminal
SEXUAL ABUSE			YES
UNCONTROLLED ACCESS OF STREET PEDDLERS		YES	
ACTS OF VANDALISM	YES	YES	YES
AGGRESSION			YES
ASSAULT / ATTEMPT AGAINST LAW ENFORCEMENT OFFICER		YES	YES
SEXUAL ASSAULT			YES
BOMB THREAT			YES
GENERIC THREATS			YES
WARNINGS OF PICKPOCKETS	YES		
FIGHTS		YES	YES



SECONOMICS

Types of security events	Uncivic	Antisocial	Criminal
UNCIVIC BEHAVIOR OF A SEXUAL NATURE	YES	YES	
UNCIVIC BEHAVIOR OF A XENOPHOBIC NATURE	YES	YES	
ALCOHOL OR OTHER DRUGS CONSUMPTION	YES		
DRUG CONSUMPTION IN PUBLIC PLACES	YES		YES
HANDING OUT FLYERS OR ANY OTHER TYPE ADVERTISING	YES		
ENTER IN TRACKS AREA	YES		
ELUCIDATION OF EVENTS THAT OCCURRED OUTSIDE	YES	YES	YES
SCAM		YES	YES
INDECENT EXPOSURE	YES		
SLEEPERS DETECTION	YES		
MUSICIANS DETECTION	YES		
TRAMP DETECTION	YES		
SMOKING ON TRAINS OR IN FACILITIES	YES		
PETTY THEFT			YES
ARSON			YES
INFRINGEMENT OF ARMS REGULATION	YES		YES
THROWING OBJECTS ON THE TRACKS	YES		
IMPROPER OPERATION OF UNDERGROUND MATERIAL	YES		
HANDLING OF CARRIAGE DOOR OPENING	YES		
HAZARDOUS OR ANNOYING MATERIALS	YES		
MISSING MINOR	YES		
ANNOYANCE / UNCIVIC BEHAVIOUR AFFECTING PEOPLE	YES		
OPEN STATIONS' EMERGENCY DOORS	YES		
PAINTED GRAFFITI	YES	YES	
PAINTED WITH ACIDS GRAFFITI			YES
MURAL GRAFFITI		YES	YES
UNAUTHORIZED PRESENCE OF ANIMALS	YES		
SCRATCHES			YES
DOING BODILY FUNCTIONS	YES		
ROBBERY WITH FORCE			YES
ROBBERY WITH VIOLENCE AND INTIMIDATION			YES
REMAIN IN FACILITIES OUT OF OPENING HOURS	YES		
TENTATIVE HOMICIDE			YES
ILLEGAL TRAFFICKING / POSSESSION OF NARCOTICS			YES
BREAKING OR DISABLING METRO COMPONENTS	YES	YES	YES
BREAKING ACCESS DOOR PAIR	YES	YES	YES
BREAKING GLASS OF FIRE EXTINGUISHER CABINET	YES		
FOUND ITEMS OF SPECIAL CARE	YES		
MISUSE OF ALARM APPLIANCES	YES		
GENERIC HAWKERS	YES		
CD, DVD, ETC. HAWKERS	YES	YES	YES
TRAVEL WITH UNAUTHORIZED ITEMS	YES		
TRAVELING IN INAPPROPRIATE PLACES	YES		
TRAVELLING WITHOUT TRANSPORT TICKET	YES	YES	YES

Types of security events	Uncivic	Antisocial	Criminal
DOMESTIC VIOLENCE			YES
Others	-	-	-
Total	36	14	26

In the first version of the requirements, countermeasures were classified in two dimensions (punitive and preventive) as they described actions that could be taken only by the public transport operator. The following categorisation goes beyond the operator itself, as it encompasses actions that fall in the scope of transport authority and/or policymakers, where they can conduct these proactive measures that can materialize in long-term preventive measures. Countermeasures are then classified as proactive, preventive and reactive to cope with the previous incident typologies described, as already put forward by some authors in the security field when dealing with the approach to public security and security risk management in its widest definition [3] [4].

Proactive countermeasures are based on the forecast of future scenarios, not yet occurred, which can show up and affect the service in a greater or lesser degree, but it is necessary to have foreseen and prepared a set of preventive and reactive measures to cope with the risk once it has shown up. An example of proactive countermeasure against counterfeit of transport tickets would be the deployment of additional security measures or the evolution towards new technologies like contact-less tickets.

Preventive countermeasures are based on the analysis of data from events that have already occurred, from which statistics, comparisons, data associations and metadata are extracted, which allows the extrapolation of trends and predictable behaviours that help decision making, resources optimization and prevention of future events as they have already happened in the past. An example of preventive countermeasure would be in the case of counterfeit of transport tickets, improving the security measures and control of tickets in the production sites and in their supply chain.

Reactive countermeasures are those that are carried out in the short term once the risk has already been shown. These measures do not need to be improvised, moreover, all of them have been planned and anticipated in internal procedures and protocols, but are applied, in any case, once the risk has already occurred. Reactive countermeasures goals are to deflect, minimize, improve knowledge or avoid the consequences of the incidents. Some examples of reactive countermeasures are the optimization of human resources to move about depending on the type of incident, the severity of the facts or the number of offenders, or not driving trains with graffiti. All these countermeasures are enforced with the aim that the damage / injury to persons (users or employees) or facilities being the smallest, besides being repaired, replaced or compensated.

Below are some examples of security countermeasures:

- new tickets technologies, contact-less (proactive);
- Detecting damaged elements of the station (reactive);
- Not driving trains with graffiti (reactive);

- Broadcast of messages on train / stations PA systems³ to prevent against criminal acts (preventive);
- Broadcast of informational / instructional videos on pickpockets / abandoned objects / suspicious objects (preventive);
- Optimal distribution of video surveillance cameras (preventive);
- Presence of security guards in hot spots of the Metro network (preventive);
- Improve the building elements and design of areas in stations in which the sense of insecurity is high (proactive);
- Improve basic training and retraining of outsourced security personnel (proactive);
- Improve communication processes of incidents (proactive);
- Improve collection information of events to assist later analysis (preventive).

With regard to the applied countermeasures, one good example is represented by the different kinds of campaigns through the Operator's communication channel or through public media. [5] [6] [7] [8]

Campaigns are carried out in a logical sequence between the public transport operator and the customer; the ultimate goal is to achieve greater transparency in the degree of knowledge and involvement that society has about uncivic, antisocial and criminal facts.

Considering purpose, audience and types of situations on which they act, there are three types of campaigns.

1. Information campaigns.

This type of campaigns is essentially preventive. Broadcasting advices prior to reactive actions (imposition of complaints) promote good behaviour fearing social reproach, avoiding its negative effect on the sense of security, particularly suitable to uncivic incidents.

Normally they should contain a general message to thank customers who behave civilly and serve as a reinforcement to continue behaving that way. After all, it should be valued that fortunately those who behave in an uncivic way are a minority, but their behaviour impact the majority. Therefore, the target of the campaign must be fully identified, informing customers that it has been detected an uncivic behaviour and that it is actively working against it.

These campaigns are developed exclusively through Operator own means of communication, PA system, Metro TV. As an example, campaigns that use these communication resources are those addressed to fight individual fraud, to prevent users accessing the track area, etc.

2. Communication campaigns.

³ Definition can be found in ANNEX 3. Glossary

This type of campaigns is basically used as a reactive countermeasure. Communication campaigns to raise users' perception about some phenomena that affect them directly and that may harm the quality of the service offered by the Public Transport Operator. These campaigns can be launched through Operator's communication means (metro channel), but they must be followed up and completed by communication strategies through public media.

Examples of this kind of communication campaigns are: to inform customers that the service has been stopped by an intrusion of graffiti writers; to inform about the economic consequences of a massive counterfeiting of tickets; to counteract the use of social networks in real time to issue slogans to commit fraud, etc.

3. Awareness campaigns.

This type of campaign is used as proactive and preventive tool. Efforts are made in raising customer awareness to bring a necessary and sufficient knowledge so that they can actively participate in the prevention of criminal acts, informing the Operator or the law enforcement forces.

In these campaigns asking for direct collaboration against uncivic acts should be avoided, as these activities are more questionable and can turn the campaign against the Operator, generating distrust if the Operator does not react as the user expects. In these cases it is highly advisable to perform some previous information and awareness activities to make it more easily accepted by public opinion.

While performing these campaigns, it is important to remember that the vast majority of people who use public transport are not uncivic, antisocial or criminal, but rather the opposite. This must be taken into account during the campaign design, avoiding the perception that the operator makes the users responsible for the solution of the problem.

These awareness campaigns should address directly public transport users, as the most affected target. These campaigns should be consistent with those made on the street, and they also should consider potential users who do not use public transport for safety reasons, justified or not.

An example of this type awareness of campaigns would be those performed to focus on the pickpockets victims' as explained in the **Scenario D: Pickpockets**. In section **Error! Reference source not found.**

2.1.3 Security objectives of TMB

The two main security objectives are the collaboration with the Law Enforcement Forces (as an available tool to and for public security) to strengthen the objective security in the public transport, and the improvement of customers' subjective feeling of security [9] [10], since the effects arising from the subjective feeling of security have a significant impact on the business of the company.

The subjective feeling of security is the most worrying for a public transport operator, as it can be crucial for a user when he decides whether to use public transport or not

[11]. Additionally, security perception is an area where the operator has full responsibility, as he manages environmental factors, and he is also competent to deal directly with annoying behaviour affecting the service or passengers (uncivic behaviours). The subjective feeling of security is also dented with criminal acts taking place in the Metro network, although in this case the security forces are responsible for facing them, as in any other part of the city.

Every Metro passenger has his own perception about objective security, but his previous experiences may provide him a greater or lesser subjective feeling of security.

The causes that impact negatively the subjective feeling of security are mainly those that affect the user's perception:

- Lack of cleanliness
- Lack of lighting
- Lack of information
- Poor attitude of security staff (lack of reaction or response to immediate situations)
- Lack of measures to eliminate security problems

Both previous objectives feedback each other, encouraging private and public security actors to collaborate and work jointly as described below:

- Collaborating with the Law Enforcement Forces to improve objective security indicators, reducing:
 - vandalism acts (antisocial behaviour)
 - mural Graffiti on trains
 - pickpocketing (criminal)
- Improving customers and non-customers subjective feeling of security, by:
 - Performing intensive operatives with Ticket Inspectors in line transfers, stations or on board. (uncivic behaviour)
 - Performing quick corrective maintenance of vandalized items
 - Avoiding the presence of pickpockets in the facilities. (criminal behaviour)
 - Keeping station clean and well lit
 - Improving collection of information to be transferred to Law Enforcement Forces
 - Providing communication land lines continuously available to users (emergency buttons in hallways, platforms and trains)
 - Limiting the number of uncivic behaviours (presence of sleepers, musicians, groups of people consuming alcohol and other drugs, etc.)

When we talk about security in public transport, it is not enough to analyse the risks, it is also convenient to provide enough information to users regarding threats and incidents that may affect them. This premise is often forgotten, even among those who have the responsibility to provide this essential service to citizens. A customer receiving a good service (punctuality, comfort, reliability ...) is a satisfied customer, if he also feels well informed when required, he becomes a secure customer. In terms of service, this is the main responsibility of a transport operator, this sense of security results in a sense of calmness that permeates throughout the transport network. [12]

As the influence of public security in the public transport is something that nobody questions today, the physical security of the users must be ensured, and this is closely linked to the technical safety of the equipment and operation of the transport. Only if technical safety is guaranteed, there will be the required conditions for public security exist.

Along with the already defined two dimensions of security, perception of security and objective security, there is a third dimension, which currently has a growing role that is related to security scenarios with social causes. This dimension comprises those incidents that, although sometimes may seem to be performed by spontaneous individuals, clearly correspond to new and complex organization and planning mechanisms. A pattern is often detected in this type of incidents, a clear disdain for society, damaging facilities to produce an economic loss and trying to break social cohesion by ignoring or neglecting living conditions and behaviour standards. This dimension has a major influence in security incidents covered in some of the scenarios described in section 4.1, like graffiti, collective and inductive fraud and scam/counterfeit for vindictive purposes.

Figure 1 shows the relation between the different security actors working jointly to provide security with passengers at the core. This picture shows that any action regarding security should have at its core the passenger, and then, the service. The operator's staff, the security staff and the external responders (Police) are covering all parts of the organization to guarantee the whole security. **Error! Reference source not found.**

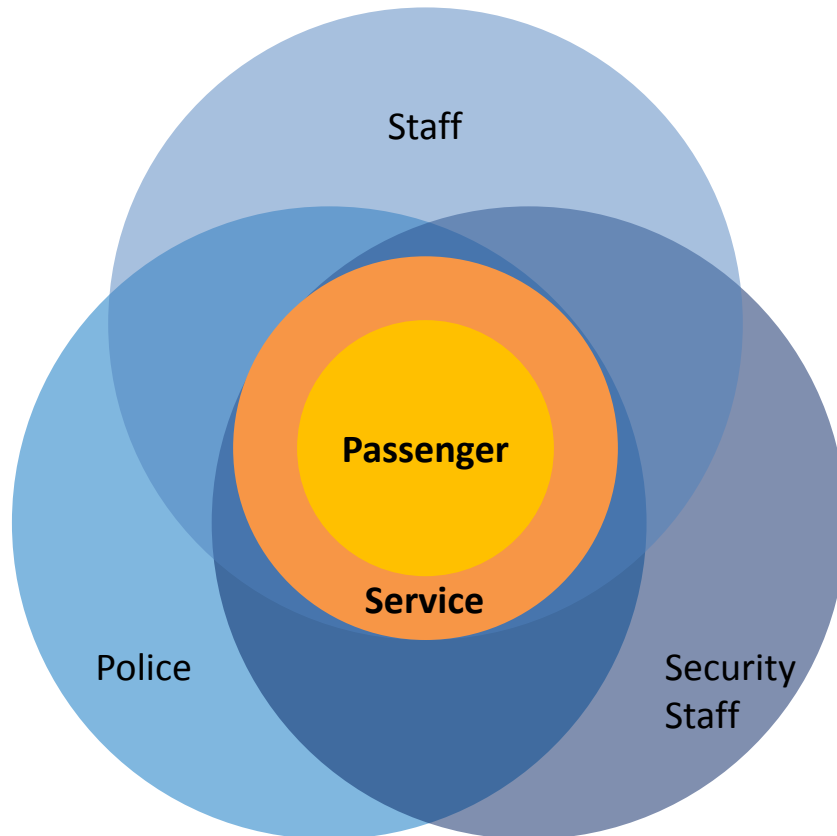


Figure 1. Relation between security actors

As a conclusion, when considering and establishing plans to tackle security issues, an operator should mainly focus on everything that affects the user's subjective feeling of security. This is because the security forces have little or no competence in this area. How would citizens feel if Police forces were dedicated to monitor fraud in Metro station access? Many would consider that to be disproportionate, and they might think that their taxes should be spent on other functions more related to the city's security, not fighting against a company's fraud.

2.1.4 Security measures of TMB

The security measures used in TMB are applied in three different planes, human, procedural and technical, using different types of resources.

The human resources provide support to the following security measures with the use of one or more combined resources:

- Early detection and reporting of security incidents
- Incidents prevention
- Surveillance
- Fraud prevention and detection
- Prevention of graffiti in train depots
- Improvement of the sense of security
- Detection of explosives

The procedural resources provide support to the following security measures:

- SOS passengers support
- Fraud detection
- Reporting of administrative offenses

The technical resources provide support to the following security measures:

- Deterrence of criminal acts and / or administrative offenses
- Police investigation
- SOS passengers support
- Passengers information on safety instructions or security incidents

The following tables, from Table 2 to Table 4, list the different types of security resources which provide the security measures listed above. Further description of the security resources and the security measures they support can be found following the tables:

Table 2. Security Human Resources

Human Resources
Solo Guards
Patrols
Anti-fraud guard
Mobile Patrols
Security dogs
Sniffer dogs
Supervisors
Ticket inspectors (employees)

Table 3. Procedural Security Resources

Procedural Resources
SOS calls
Revisions of tickets by Ticket inspectors (employees)
Administrative complaints

Table 4. Technical Security Resources

Technical Resources
Video surveillance cameras
On board video surveillance cameras
SOS Intercoms
PA system in station
Metro TV in station

A. Human Resources:

All security staff carry the operator logo on the back of the uniform of their company, in addition to the logo of the private security company to which they belong. This fact makes the users consider security guards to be specialized and sensitive with Operator's own environment. Furthermore, this also increases loyalty of the security guard towards the operator, which is very positive for the perception of the security guard on the role he plays within the Operator, above and beyond the service that his company provides to the Public Transport Operator.



Figure 2. Security Guards' Uniform (source TMB)

In addition, the upper part of the security guards' uniform is made of orange reflective material with photo luminescent bands (certified high visibility garments). This element increases security guards' visibility and therefore their presence in front of users, enhancing their sense of security.

Furthermore, all security staff carries the same backed-up communication equipment. This equipment allows them to contact the Security & Civil Protection Centre, from where they are coordinated, and other security guards located in the same metro line in case they need urgent reinforcements.



Figure 3. Security & Civil Protection Centre (source TMB)

To manage security incidents and take into account their different severity and impact on service and users, different types of security services are used. Those services are tailored to provide the best possible response according to the circumstances and the characteristics of each security incident. Such services are the following:

1. Solo guards [13]:

Security guard that starts, develops and ends his service alone, and may be supported by other teams in case of incidents. His main function is to provide early detection and reporting of Security and Civil Protection



incidents while he covers some routes and operatives specified by the Transport Operator. His main tools are the proximity perception, his proactivity and the required skills to manage conflict in a proportionate manner.

This type of service was a great novelty when it was established in 2004. At the beginning it produced some typical opposition from reluctance to change, but finally it has reduced attacks to security guards. In addition it was found that to approach a lone security guard was less intimidating than a security guard patrol.

2. Patrols:

Figure 4. Solo guard (source TMB)

Couple of security guards whose main function is to support the solo guards and other types of security officers or employees, attending incidents that cannot be managed by them or require more human resources for its complexity or dangerousness.

3. Anti-fraud guard:

It consists in a solo guard mainly intended to prevent fraud. It is located behind the ticket validation area in those hallways where, after observation and analysis, a high fraud rate has been detected that justifies such recruitment and presence of a security guard. The anti-fraud guard can be required by the Security & Civil Protection Centre to attend other incidents.

The static nature of this service, jointly with the condition of working in isolation, makes selection process particularly important, as it requires a profile highly suitable to the requirements of the service to avoid poor actions or performance of the service.

4. Mobile Patrols:

Vehicles composed by two security guards allocated on the street, outside the metro network, to protect other facilities and network access points not in use. Their main goal is to prevent graffiti mural in train depots (suburbs). Their mobility and speed are very useful to face incidents that cause train traffic stop (track area intrusion, derailments, technical failures, etc.) as a result of technical or security and civil protection issues.

5. Security dogs:



Figure 5. Security guard and dog (source TMB)

It is a team composed by a security guard, qualified to handle trained dogs, accompanied by a security dog with muzzle. This type of team is particularly aimed to improve the sense of security, because the impact caused by the presence of dogs, they are very deterrent in certain incidents in supporting other safety teams.

It also allows the availability of sniffer dogs, but not directly associated with alarm conditions by the presence of suspicious objects that may eventually be prohibited or dangerous materials (explosives).

6. Sniffer dogs:

Security guards, qualified to handle trained dogs for explosive detection, accompanied by a dog without a muzzle trained specifically for the detection of explosive material. This type of team is focused, almost exclusively, to check objects which by their nature or location require caution in their management, so before they are moved, should be reviewed by this type of security guards.

With this service, TMB and security staff get used to keep patterns of caution in the management of abandoned objects, which in normal situations, and specifically during on alert situations, can help to manage risks in a more secure and professional way. In this sense, it should be emphasized the importance of having done a previous training work, very important when they are urgently required to face an emergency situation of maximum public sensitivity.

7. Supervisors:

Inspectors or security guards with a higher hierarchical rank serve as managers and supervisors of a given group of security guards, because of their location or type of service.

Supervisors are responsible for realizing the technical and organizational responsibility of security companies on security guards, in this way they provide training on a daily basis, deliver operating materials, fix some actions, ensure coverage of all services, and, on some occasions, not for operational issues, act as spokesperson with the Security & Civil Protection Centre.

8. Ticket inspectors (employees):

TMB employees dependent from Security & Civil Protection Unit whose main function is to check for the existence and validity of the greatest number of users' tickets, with a twofold objective: (1) that the user who has properly validated his ticket perceives a sense of control and performance by the operator, although he has seen other people committing fraud before him. (2) The user who has committed fraud is administratively reported and do not see profitable doing it in the future.

Along with security guards anti-fraud is the main tool to curb the rising trend of fraud. While anti-fraud guards made a correction on site, with a reactive service planning, the interventions carried out randomly and continuously by ticket inspectors respond to a prevention and deterrent purpose, which achieves a high impact, have longer term effects and a more general nature.

B. Procedural Resources:

1. Treatment of SOS calls:

There is a network of intercoms spread all over the transport network which are the entry points for SOS calls (detailed in the next section C. Technical resources). On average 12.000 calls per week are recorded (only 1% are actually emergency calls, the others are errors, involuntary calls, equipment check, or malicious), all of them are answered, with an average response time of 3,5 seconds.

These calls are answered by the Security & Civil Protection Centre, using a computer application that records all information relevant to the management of the incident that triggered the call, as well as for further analysis. The application can record calls; this allows the calls to be played back in a few seconds. It enables detection and analysis of some parts of the conversations that often, while listening in real time, are difficult to appreciate.

2. Revisions of tickets by Ticket inspectors (employees):

The traditional inspection work has been enhanced and driven with procedural measures, such as conducting intensive interventions, where both advance information to clients and the proper driving of passenger flow, speed up the process.

3. Administrative complaints:

Administrative complaints are a legal tool by which the public transport operator informs competent authorities of certain behaviour performed by a user and typified as infraction in the traveller regulations.

The administrative authority may be carried out by law enforcement agents who serve the Public Transport Operator, whether they are own employees or hired security guards, according to current legislation.

Administrative complaints lodged by employees (mainly by Ticket inspectors) are driven by the commission of fraud. However, complaints registered by security guards are more heterogeneous, denouncing not only detected fraud, but uncivic behaviour (users who disturb, annoy, carry over-sized items, soil facilities, etc.) and antisocial behaviour (users who deteriorate trains or facilities-graffiti-, break metro elements -extinguisher glasses, doors, windows, etc.)

In certain cases, there is a fuzzy border between the administrative complaints and the criminal charges that the public transport operator must perform, allowing the operator to choose if it prefers to start administrative or criminal proceedings. Even though, both tracks cannot be activated simultaneously, because it would violate the constitutional principle of double jeopardy (*non bis in idem*).

The decision to undertake criminal complaint in view of certain behaviour that has produced economic harm to the Operator depends on several variables:

- The behaviour is classified as an offense or crime in the Criminal Code;
- It was an uncivic behaviour;
- The consequences of the behaviour are serious or very serious (one criterion may be that the repair or replacement value is greater than 400 €, the Spanish legal reference for distinguishing misdemeanors from crimes);
- The perpetrator or perpetrators of such conduct are identified or identifiable after investigation (identifying pictures on video recordings, witnesses, etc..).

Certainly, the possibility to complain administratively for particular less serious behaviours is very useful and efficient compared to the criminal complaints that, in addition to Operator's internal human resources, involves the mobilization of police who collected the complaint, lawyers, prosecutors, judges and witnesses of the events. This mobilization of human and technical resources is not proportional to deal with particular behaviours that can be addressed administratively in a faster way.

C. Technical Resources:

1. Video surveillance cameras in facilities and on board (CCTV):

Over 4500 surveillance cameras are installed throughout the facilities and 1800 cameras on board of trains. Historically, the criterion for the installation of a camera has been to make easier the management of the traffic and the passage and / or detect the origin of certain technical problems.

Later on, and particularly after the terrorist attacks of March 11, 2004 in Madrid, it has been giving more importance to security criteria, installing cameras in locations where they can help deter criminal acts and / or administrative offenses or clarify these same facts, whether the Operator itself or with the help of the law enforcement forces.

In addition, this technical resource is permanently used by Law Enforcement Agencies to investigate multitude of facts, including facts not occurred in the facilities nor related with the Operator itself, to obtain images to identify people related with these facts who have used public transport, which help research and fact-finding.

2. SOS Intercoms:

Throughout the entire transport network some vertical and showy TOTEMS are strategically

D3.3 Urban public transport requirements fir



located, by means of which the user can report any incident that he is witnessing. These TOTEMS are located in hallways, line transfers and platforms: they are a reference of permanent communication between the user and the Security & Civil Protection Centre and they can significantly increase the sense of security, especially if there are no employees or security guards at the time and place in which something happens. In addition to the strategically located TOTEMS, there are SOS intercom buttons in all carriages of each train, so that users can contact an employee immediately to report any incident that is occurring.

Figure 6. SOS Intrecom totem (source TMB)

3. PA system in station:

In all stations (hallways and platforms), as well as in all trains, there is PA system through which all kinds of messages are issued, security messages included. With respect to safety, the PA system is used for periodic broadcast of pre-set messages, either on safety instructions regarding pickpockets or personal property, or messages about security incidents and civil protection, for example the case of a line stop caused by an intrusion of graffiti writers in track area. It is a good tool for issuing information campaigns, communications and raising awareness.

4. Metro TV:

As with the PA system, screens and projectors distributed across all platforms and trains are used to issue videos on different security topics. In the case of Barcelona, videos are broadcasted on pickpockets and unattended vs suspicious objects, and they give concrete instructions to users detecting these incidents.

2.2 Risk prevention framework at TMB

The risk prevention framework in TMB is based in procedural as well as in organizational tools, which consider the different dimensions of the security scenarios, using the information collected by the transport operator related to security incidents, and the perception of security by transport users.

This framework considers, as a first step, the analysis of all the environmental factors that influence the customer's subjective feeling of security and also, all incidents and behaviours' which harm or disturb the service or the passengers, objective security.

The analysis of the information collected by the public transport operator regarding security incidents provides the main input to set-up action plans, which must be addressed and coordinated across the different public transport operator areas.

TMB follows closely the evolution of incidents which affect the subjective feeling of security. This is performed through a management tool, called "Segurómetro"⁴. This tool

⁴ Definition can be found in ANNEX 3. Glossary

is used to analyse the evolution of both, perception of security and objective security. Based on the information provided by this tool, private security services are deployed following the operating guidelines defined by the operator. Law enforcement agencies work closely with the operator's security team, periodic coordination meetings are scheduled for coordination and exchange of information with police unit, specialized in public transport (Mossos d'Esquadra - Divisió de Transport).

The following tasks are performed by the operator's security department:

- Coordination of services;
- development of security procedures;
- internal and external communication;
- development and monitoring of action plans.

This department is called "Unitat de Seguretat i Protecció Civil" (USPC; in English, Security and Civil Protection Unit), and it is composed of three departments: Anti-Fraud, Security and Civil Protection. A monitoring and permanent supervision body has special prominence, the Centre for Security and Civil Protection (CSPC), allowing the coordination of all services and the management of all incidents that occur. This has a significant number of people and use complex technological systems which are in constant evolution.

The organization of the USPC is described in Figure 7:

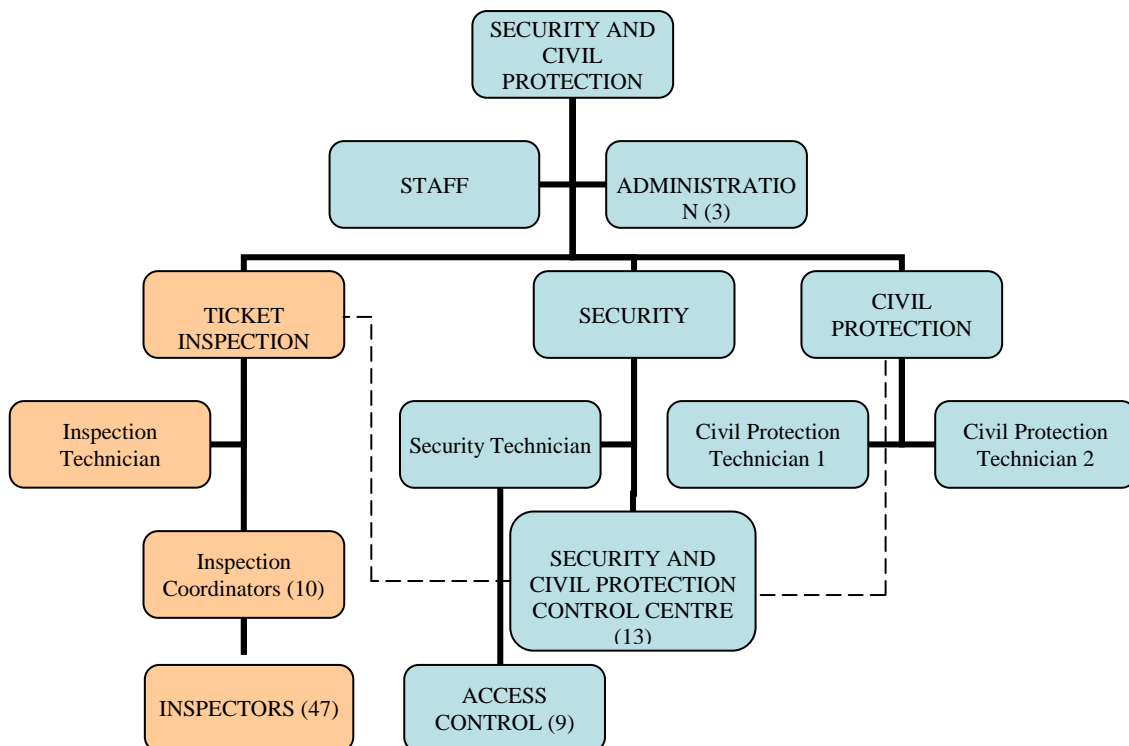


Figure 7. Organization chart of the Security and Civil Protection Unit (source TMB)

The operation of the USPC is based on the ability to manage incidents with the least possible effect on transport service. It is subject to a quality control system shared with other units and departments to support the service.

2.3 Regulatory framework for underground urban transport

At European level, DIRECTIVE 2004/49/EC -Railway Safety Directive- [14] is the closest regulation to passenger's railway transport. It applies to railway systems with the exception of Metros, trams and other light rail systems, as they are subject to local or regional safety rules, and supervised by regional authorities. Therefore urban transport is not affected by EU regulations. This is explicitly detailed in Article 2 of the Directive "Scope" [14].

In the case of Barcelona such competences are transferred to the regional government who has issued the corresponding Law regulating the railroad transport. Regarding security, it focuses on infrastructure safety and basic passengers' duties and rights. In addition, each operator is responsible for issuing its passengers' regulation based on the framework defined in the previously mentioned Law. This regulation is more specific about passengers' security and safety.

The specific Transport regulations for the Barcelona public transport can be found at TMB web site, under "Your transport / Customer services / Using public transport / Regulations", <http://www.tmb.cat/ca/legislacio-de-transport>

Specifically:

- Regional Law regulating the railroad transport in Catalonia: Law 4/2006, of 31 March, on railways: This law regulates railways services, and the rights and obligations of passengers (Title VIII), and categorises infractions (Title X) [15].
- General terms and rules of use of Ferrocarril Metropolità de Barcelona, SA, metro service: Regulation for passengers of Ferrocarril Metropolità de Barcelona [16].

2.4 Description of Xarxa4

The security measures in Xarxa4 - which is the portion of the Barcelona network being considered for the scenarios described in this report- are equivalent to those applied to the whole Metro network, with a variation in the amount of resources allocated, as it is reported later in this section.

So data and conclusions can be extrapolated, since Xarxa4 is the central part of the Metro network. More detailed information about the context of Xarxa 4 in relation with the whole Barcelona network can be found in *ANNEX 1. Xarxa 4 in the context of the Barcelona metro network*.

2.4.1 Resource distribution in Xarxa4

Besides other secondary parameters, the geographic distribution of stations or the number of passengers in each station can be used to calculate the best resource optimization over the network according to each need and risk.

According to available data from 2011, the passage of Xarxa4 represented 22,5% of total validations in the Metro network, as can be seen in Table 5:

Table 5. 2011 total validations and passengers (source TMB)

Ticket Validations 2011	Total/Yearly Network	Total/Yearly Xarxa4
Approximate number of total users (individuals) (60% of validations)	233.389.373	52.633.186
Total ticket validations	388.982.289	87.721.976

Moreover, the metro stations in Xarxa4 represents 12,1% of the entire Network as it is composed of 17 stations of the 140 stations that are available [1].

In 2011 33,69% of all security incidents took place in Xarxa4, which is located in the city centre and therefore the centre of the transport network. The resources to be allocated in Xarxa4 must be necessarily higher than those devoted to the rest of the transport network, according both to the number of passengers and the number of incidents.

In relation to the type of security services, the distribution of resources in hours would be the following, as presented in Table 6:

Table 6. 2011 security resources distribution in Xarxa4 vs. Network (source TMB)

Human Resources	Total/Yearly Network (hours)	Total/Yearly Xarxa4 (hours)	% Xarxa4 vs. Network by stations
Solo Guards	256.702	36.049	13,55
Patrols	229.246	21.230	20,23
Anti-fraud guard	98.662	17.463	17,73
Mobile Patrols	39.225	1.430	1,90
Security dogs	62.458	13.169	20,24
Sniffer dogs	5.854	52	0,93
Supervisors	39.385	9.953	23,48
Ticket inspectors (employees)	55.378	4.577	8,26
Procedural Resources	Total/Yearly Network	Total/Yearly Xarxa4	% Xarxa4 vs. Network by stations
No. of SOS calls	679.752		
Total revisions of tickets by Ticket inspectors (employees)	4.066.942		
No. of ticket revisions by Ticket inspectors per hour	73		
No. of administrative complaints (employees)	65.293		
No. of administrative complaints (Security Officers)	5.640		
Technical Resources	Total/Yearly Network	Total/Yearly Xarxa4	% Xarxa4 vs. Network by stations
No. of video surveillance cameras	4.599	512	11,13
No. of on board video surveillance cameras	1.828	250	13,68
No. SOS Intercoms	1.589	105	6,61

PA system in station	100%	100%	100%
Metro TV in station	100%	100%	100%

Xarxa4 accounts for 12,1% of the total network stations. The rightmost column of Table 6 shows the percentage of time spent by security resources in Xarxa4, where green cells are for resources spending a percentage of time above the percentage of Xarxa4 stations vs. all network stations; orange is for resources which spend a percentage of time aligned with the percentage of Xarxa4 stations; red is for resources which spend a percentage of time below the percentage of Xarxa4 stations.

Therefore, almost all security services spend proportionally more time in this area, except:

a. Mobile Patrols:

They are primarily allocated to prevent suburban network intrusion in non-enabled access points and graffiti mural in train depots, avoiding the city centre due to the traffic conditions there during the day.

b. Sniffer dogs:

They must often intercept trains in which unattended objects, that require minimal care in their management and treatment, are found, and performing this activity in locations where the impact on the service is minimized (railway sidings, line endings or workshops). For this reason their presence in Xarxa4 is not very high. There is no service level agreement for these types of services, but there is a strong interest in getting shorter waiting times when these services are performed in the central part of the network, where vulnerability and impact represent a greater risk probability. Therefore, it is more than possible that in the near future the percentage of presence in the area covered by Xarxa4 (not at stations, by the nature of the service) will be significantly increased.

c. Ticket inspectors (employees):

Intensive ticket inspections are performed in peripheral line transfers, since most passengers come to the city centre from the suburbs, being equally effective and surprising performing ticket inspections halfway or at the end.

In contrast, Individual Guards, Patrols, the Anti-fraud guards, Security dogs and Supervisors, spend many more hours in the centre of the line than in other locations, primarily because of the number of incidents and the amount of passengers.

It should be noted that there is a computer application that analyses and integrates all information obtained on fraud (complaints of all employees and security guards, fraud data extracted from the validation gates...) to designate routes and points where intervention teams will do their work.

2.4.2 Distribution of incidents in Xarxa4

There is not a proportional distribution of incidents occurring in Xarxa4 in relation to the remainder of the network, due to the fact that Xarxa4 is located in the centre of the



metro network. Not all the types of incidents have a homogeneous distribution according to its nature. For example pickpockets occur more often in the most crowded stations, usually visited by tourists, but almost with no incidents in the most external branches of the network. In contrast, certain types of graffiti incidents occur more often in the railway parking areas, usually located at the end of metro lines.

3. Stakeholders & Engagement Plan

In SECONOMICS D3.2, in which the first version of the requirements was reported, some specific stakeholders for the Barcelona urban transport were identified. Hereafter the plan for their engagement during the different project phases will be outlined.

In the following Table 7, we propose a rearrangement and classification of stakeholders defined in D3.2, defining their main roles in relation to the security aspects of the urban transport, in order to properly plan their participation during the SECONOMICS project life.

Table 7. Barcelona urban transport stakeholders

Stakeholder type	Barcelona urban transport's stakeholder	Main roles
Users	<ul style="list-style-type: none"> • Neighborhood associations • Public transport users associations • Consumers organizations 	<ul style="list-style-type: none"> • The main concerns of the user's representatives are mainly related to the service quality, the annual review of fares, and the promotion of mobility. Security issues are often at a secondary level, and often used as a way to put pressure on the main issues.
Public authorities and regulators	<ul style="list-style-type: none"> • Regional government (Generalitat de Catalunya) • Barcelona Metropolitan Area (AMB - Àrea Metropolitana de Barcelona) • Metropolitan Transport Authority (ATM - Autoritat del Transport Metropolita) 	<ul style="list-style-type: none"> • Regional government has the competences for the regulation of the railway sector. In turn it is also the holder of the infrastructure operated by TMB. • Barcelona Metropolitan Area organization has the competences for the provision of underground public transport on behalf of the municipalities that comprise it. • ATM has many competences, among them setting the tariffs and future regulation framework
Urban transport operators	<ul style="list-style-type: none"> • TMB (Transports Metropolitans de Barcelona) • Ferrocarrils de la Generalitat de Catalunya • RENFE Rodalies • TRAM Baix & TRAM Besòs 	<ul style="list-style-type: none"> • Is the operator of the underground public transport and responsible for its security • Other railway system operators in the Barcelona area, that also have security issues and requires some coordination with.
Other Urban transport operators	<ul style="list-style-type: none"> • UITP - International Association of Public Transport 	<ul style="list-style-type: none"> • The UITP Commission on Security seeks to study, assess and promote innovative operation and technology for enhanced Public Transport Security
Law enforcement agencies	<ul style="list-style-type: none"> • Regional police (Mossos d'Escuadra) 	<ul style="list-style-type: none"> • Provide assistance under requirement of operator employees
First responders	<ul style="list-style-type: none"> • Medical Emergencies (SEM - Sistema d'Emergències Mèdiques) • Barcelona Fire Service • Generalitat Fire Service • Civil Protection 	<ul style="list-style-type: none"> • Provide emergency support under the requirement of operator employees

Stakeholders' engagement per phase

For each stakeholder type described above, a proposal for participation and involvement is presented for the following three project phases:

- Definition of requirements phase: Requirements collection and its validation;
- Model validation phase: Assessing the urban public transport security model produced in its three aspects; social model, risk model and economic model;
- Tool validation phase: Support the tool validation process.

Users: Given the background experience with users' stakeholders, the most appropriate seems to encourage their participation during the model validation phase, more specifically in the social model and, in a lesser extent, in the risk model validation. Therefore it is considered the most appropriate to disseminate project outcomes among user stakeholders during the model validation phase, and then collect their inputs.

Public authorities and regulators: Public authorities and regulators can provide model and tool validation as they must be aware of economic and social impacts of regulations. As far as they do not deal with day to day operation are not much aware of all the security-related requirements.

It seems the most appropriate to disseminate project outcomes among user stakeholders during the model and tool validation phases and then collect their inputs.

Urban transport operators: Local operators in the same area where TMB operates. They can provide inputs for requirements and validation of models and tools, as they deal with these issues on a day to day basis. Operators are involved during all project lifecycle with corresponding dissemination activities and also gathering of their significant inputs.

Other Urban transport operators: Operators from other cities and countries. Their participation is similar to the local ones. They will be involved during all project lifecycle with corresponding dissemination activities and also gathering of their significant inputs.

Law enforcement agencies: As organizations that deal with crime and security, they can provide significant inputs during the requirements and model validation phases. These agencies are involved from the requirements phase with corresponding dissemination activities and also gathering of their significant inputs.

First responders: As organizations that deal with emergencies, often caused by criminal actions or incidents related with the security, they are also able to provide significant inputs during the requirements and model validation phases. Corresponding dissemination activities are carried out during the requirements and model validation phases.

The following Table 8 summarizes the engagement plan for each stakeholder type according to the descriptions made above of each stakeholder engagement.

Table 8. Stakeholders engagement per type

Stakeholder type	Requirements Definition	Model validation	Tool validation
Users		✓	
Public authorities and regulators		✓	✓
Urban transport operators	✓	✓	✓
Other Urban transport operators	✓	✓	✓
Law enforcement agencies	✓	✓	
First responders	✓	✓	

Detailed engagement plan

The Table 9 below shows the stakeholders' engagement activities to be carried by WP3 during the project lifecycle.

Table 9. Stakeholders' engagement activities plan

Y1	Requirements Phase		
	M1-M3	M4-M6	M6-M12
	Stakeholders Identification and Preliminary Contacts-	Presentation of use case goals to urban transport stakeholder (TMB) and Law enforcement agencies	Presentation of first version scenarios to urban transport operator stakeholder (UITP) Review with End User Partner
Y2	Model validation phase		
	M18-M21	M22-M24	
	Presentation of first version of models to selected stakeholders (†)	Presentation of final version of models to selected stakeholders (†)	
Y3	Tool validation phase		
	M34		
	Presentation of final Tool to transport stakeholders and Public authorities and regulators		

(†) With both presentations all stakeholders' types will be covered

Engagement actions so far

During the Urban Public Transport Case Study Workshop held in TMB, Barcelona, on the 7th June 2012, a project description, a use case description and goals, and a first version of scenario descriptions were presented to attendants.

Stakeholders attendance:

- Representatives from the security area of TMB;
- Representatives form the Transport division of Regional police (Mossos d'Esquadra);
- Seconomics Consortium representatives.

During the UITP Commission on Security meeting held in Munich on the 7th and 8th of November 2012, a project description, a use case description and goals, and the first version of scenario descriptions were presented to attendants.

During the closing of the presentation it was mentioned that volunteers for the Expert group are welcomed to join. It was also announced that the next Seconomics WP3 stakeholders meeting will be held at the beginning of 2013 to be attended by those joining the Expert Group.

Stakeholders attendance:

- Representatives from the UITP Commission on Security;
- Representatives from the security areas from several European underground urban transport (see following Table 10).

Table 10. Attending operators to the UITP workshop

Operator	Country
WIENER LINIEN GMBH & CO KG	Austria
LONDON UNDERGROUND LTD	United Kingdom
FERROCARRIL METROPOLITA DE BARCELONA	Spain
MÜNCHNER VERKEHRSGESELLSCHAFT	Germany
DOPRAVNI PODNIK HLM PRAHA AS	Czech Republic
REGIE AUTONOME DES TRANSPORTS PARISIENS	France
EAST JAPAN RAILWAY COMPANY	Japan
DEUTSCHE BAHN AG	Germany
HAMBURGER HOCHBAHN-WACHE GMBH	Germany
BERLINER VERKEHRSBETRIEBE	Germany
TEHRAN URBAN & SUBURBAN RAILWAY CO	Iran
ATAC S.P.A.	Italy
HTM PERSONEN VERVOER NV	Netherlands
TRANSPORTS METROPOLITANS DE BARCELONA	Spain
MOSCOW METRO	Russian Federation
MOSGORTANS	Russian Federation
MTA NEW YORK CITY TRANSIT	United States of America
UNION INTERNATIONALE DES CHEMINS DE FER	France
AMERICAN PUBLIC TRANSPORTATION ASSOCIATION	United States of America
COLPOFER	France
VDV	Germany
Metropolitano de Lisboa, E.P.E.	Portugal
UITP	Belgium

Internal validation

A process for validation of the different outcomes from the project was defined by every case study of this project in D7.1, Validation Plan. According to that plan, the validation process followed in this first phase of the project, Stakeholders Needs Identification, is described in *ANNEX 2. Internal validation*.

4. Urban transport scenarios based on current threats

4.1 Description of scenarios

This section provides a description of selected scenarios with the different typologies of incidents that apply and their application to all railway public transport at international level.

For each scenario it is provided some information in tables about the classification of the effects of the security scenario. This information is based on the data compiled over the time with the security monitoring tools, like the “Segurómetro” described in previous sections.

For each scenario it is provided some information in tables about the economic and social impact of the security scenario. The economic impact is based on information compiled based on estimations and the actual cost of security incidents. For the social impact it is based on surveys performed periodically by TMB to the metro users.

1. Scenario A: Indicators of economic crisis:

This particular scenario aims to bring together all those incidents of uncivic-social nature affecting customers’ sense of insecurity on a daily basis, that have been growing since the start of the economic crisis, like:

- Musicians
- Sleepers
- Beggars
- Hawkers

Apparently other activities like fraud and pickpockets activities may also have increased during the crisis. On the contrary, with the crisis the number of passengers has decreased, having this an impact on those fraudsters and pickpockets which have decreased their activity proportionally, as they have less opportunities to work. This is what the numbers of incidents registered by TMB is showing since the start of the economic crisis in 2009.

In Table 11 are shown the different types of security incidents covered in this scenario.

Table 11. Typology of incidents and its classification for scenario A

Incident	Typology	Uncivic	Antisocial	Criminal
Indicators of economic crisis	Musicians	YES	-	-
	Organized musicians	YES	YES	-
	Sleepers	YES	-	-
	Beggars	YES	-	-
	Organized beggars	YES	YES	-
	Single hawking	YES	-	-
	Organized hawking	YES	YES	-

This type of incident is detailed in different subgroups to itemize all objective and subjective metadata attributed to each one, based on different evaluation parameters described below.

In this scenario there are three major subgroups with monetary or economic objectives such as:

- Musicians
- Beggars
- Hawkers

, as they provide goods and services and request compensation in return.

Sleepers are the only subgroup that does not try to get any economic benefit, but they are just people with no social ties living in the streets who take refuge in the underground facilities.

These subgroups with economic objectives may have different degrees or levels of organization and planning; that makes the subjective feeling of security more or less impacted according to such organization, as shown in Table 11.

Based on the definitions of uncivic, antisocial and criminal behaviours⁵, each subgroup can be qualified. All subgroups fall in the UNCIVIC classification, and some in the ANTISOCIAL. This ANTISOCIAL aspect is the case of organized musicians, organized beggars or organized hawking, namely those subgroups that relate to actions whose means or objectives can directly affect society, taking advantage of it or going against it.

This conceptual distinction makes sense in order to adapt the technical, human and procedural resources based on the inherent characteristics of each subgroup, adapting the most effective and efficient countermeasures. In this case, a single beggar or musician does not receive an administrative complaint; he is just evicted from the station as imposing an administrative complaint is considered disproportionate and inefficient, that will surely be difficult to collect because of the most likely insolvency of these groups.

In addition, there are many cases in which part of citizenship does not share the crackdown against such behaviours, because they justify it under reasons of humanity or compassion. Instead, in some cases there is a kind of organization behind, that is, groups composed of several individuals that share out the stations and the time slots in which they operate. They also use advanced technical means (amplifiers or speakers) and / or carry out some uncivic or rude behaviour towards users. In these cases an administrative complaint is imposed and, if there are doubts about the identity of that person, police are alerted to proceed with his identification, and if required, the individuals moved to the Police Station, which greatly affects the economic objective of these individuals. In these cases, there is a clear disregard to the good faith of the people they devote to cheat in order to obtain benefits, often far away to the primary needs that they pretend to show, and usually being part of paracriminal organizations.

⁵ Definitions can be found in ANNEX 3. Glossary

Regarding the effects on the safety of incidents associated with this scenario the following descriptive Table 12 is used:

Table 12. Classification of the effects of the security of incidents for scenario A

Typology	Insecure feeling Allocation	Objective Security Allocation (0-4)	Social Alarm Allocation (0-4)	Tolerance level in number of incident per 1.000.000 users (1 day)
Musicians	LOW	0	0	20
Organized musicians	MED	1	0	10
Sleepers	MED	0	0	15
Beggars	MED	0	0	17
Organized beggars	HIGH	1	0	10
Single hawking	MED	0	0	30
Organized hawking	HIGH	1	0	10

Table 12 is composed of four columns in which it is described the impact of such incidents on users, as well as the level of tolerance that as a railway operator can be assumed bearing in mind the availability of resources and priorities in their use. Be said that all the information in this section is subjective, that is, chosen and designed by the railway operator based on their own statistics, although biased, give support to decision-making process and adaptability to changing realities and trends.

In this scenario, the effects on the sense of insecurity is medium to high, with the exception of individual musicians, because it comes directly to issues affecting the perception of control and order that the user expects in a means of transport. This rating is based on the information collected; the nature of written or verbal complaints received, and the several surveys that have been conducted in recent years, both to Barcelona Metro users and with any survey related to objective and subjective feeling of security.

Furthermore, this type of incidents does not affect the objective security, as these events are not considered to be criminal. These typologies of incidents do not generate social alarm, because of the current society tolerance, albeit with varying degrees of acceptance and nuances.

Therefore, the tolerance of the number of incidents in this case, depends on the side effects, such as dirt of the environment, noise saturation or by the exposition to bad social awareness, so that these situations are not a problem to be addressed with priority, and although quantitatively the impact may be relevant, not qualitatively affects the social impact too.

Table 13. Economic and social impact of incidents for scenario A

Typology	Economic Impact	Social Impact
Musicians	LOW	LOW

Organized musicians	LOW	MED
Sleepers	LOW	LOW
Beggars	LOW	LOW
Organized beggars	LOW	HIGH
Single hawking	LOW	LOW
Organized hawking	LOW	HIGH

As can be seen on Table 13, the economic impact is a key concept to the dimensioning of resources, in order to achieve maximum efficiency and organizational effectiveness at the operational level. Nevertheless, the economic impact of all subgroups is low, as they do not affect directly any of the business activities.

However, in terms of social impacts, as well as with the social alarm, it is significantly increased when the activities carried out clearly involve illegal profit-driven organizations. This organization and planning usually breaks the acceptance of society towards these behaviours, as it incorporates a trick to good faith that makes it incompatible with social compassion that such facts deserve. These organized activities become clearly antisocial. The connotation of social scorn that entails such conduct is the key factor to differentiate it from the individual or purely spontaneous activities.

Table 14. Administrative and criminal regulation of incidents for scenario A

Typology	Administrative Regulation	Criminal Regulation
Musicians	YES	NO
Organized musicians	YES	NO
Sleepers	NO	NO
Beggars	YES	NO
Organized beggars	YES	NO
Single hawking	YES	NO
Organized hawking	YES	YES (if it affects intellectual property)

Among the countermeasures that are carried out to counter the direct and indirect impact caused by the authors of this type of incidents, is the application of criminal and administrative regulations, as it is referenced in Table 14 for each incident. It should be recognized that there are certain behaviours for which an administrative complaint is not proportional: musicians, sleepers, beggars and hawkers are just simply accompanied outside the facilities, as an exhaustion technique. This is carefully done to do not stigmatize these collectives, so as the actions try to cope with the consequences, but not to the groups or profiles.

The only activity to be criminally prosecuted is organized hawking insofar it concerns intellectual property of a particular brand, and it is considered an offense under the criminal jurisdiction.

The key actions would aim primarily to counteract the effects that cause discomfort, such as beggars saturation of special impact (in trains, near the ticket machines ..), dirt, musicians, with regulation of time and place compatible with the service.

Regarding organized activities, the best practice is to expose to deception those who assume good faith, pretending to be spontaneous and individual. Publicize these practices would draw legal weight, acting on the causes that make them viable and profitable to those who implement them. If begging is organized and integrated into networks of exploitation of persons, not supporting them may be the best measure to prevent proliferation and to its decline. The same could happen with organized vending, often related to extensive networks of illegal immigration and labour exploitation.

2. Scenario B: Fraud:

This scenario encompasses all those typologies of incidents related to the commission of fraud which have an economic impact on the metro operation, like:

- Individual / multiple offenders
- Collective and organized offenders
- Induction to fraud
- Scam and counterfeit

The number of individual offenders has decreased with the economic crisis, as the total numbers of passenger has done too, and also thanks to the new strategies for the inspection of tickets. Collective and inductive activities have increased due the activity of some organized groups with vindictive purposes. Scam and counterfeit activities have two causes, one due to the activity of organized groups with vindictive purposes, like collective and inductive fraud, and another with economic causes.

A classification according to the typology of incidents can be found in Table 15.

Table 15. Classification of typology of incidents for scenario B

Incident	Typology	Uncivic	Antisocial	Criminal
Indicators of Fraud	Individual	YES	-	-
	Multiple offender	-	YES	-
	Collective and organized	-	YES	-
	Inductive	-	YES	-
	Scam / counterfeiting for profit	-	-	YES
	Scam / counterfeiting for vindictive purpose	-	YES	YES

It can be considered that UNCIVIC fraud is done simply when the ticket is not paid, but not disturbing any user nor promoting this type of action among other users. If this fraud becomes routine and recurrent and / or affects other users on a regular basis this should be included in the ANTISOCIAL category, like those involving organization sub-typologies (collective and organized fraud) and / or some claim (inductive protests for collective and organized fraud / forgery). Final category is for CRIMINAL incidents that are encompassed within the criminal offense, such as fraud and counterfeiting of tickets, whether profit-making or protest.

Table 16. Classification of the effects on the security of incidents for scenario B

Typology	Insecure feeling Allocation	Objective Security Allocation (0-4)	Social Alarm Allocation (0-4)	Tolerance level in number of incident per 1.000.000 users (1 day)
Individual	LOW	0	1	60000
Multiple offender	LOW	0	2	60000
Collective and organized	HIGH	0	3	2
Inductive	HIGH	3	4	0
Scam / counterfeiting for profit	LOW	4	3	0
Scam / counterfeiting for vindictive purpose	LOW	4	4	0

As can be appreciated in Table 16, fraud affects differently to the sense of security and social alarm depending on the visibility of the acts, i.e. for individual facts and discrete fraud, even multi recidivists, the effect is low, as with fraud and counterfeiting of tickets, provided that such action does not compromise other users directly (e.g. when someone commits fraud and at the same time a user validates its ticket). In these cases, it is assumed that one who commits fraud performs an action related with the inactivity or permissiveness of the "system". Therefore it is difficult to explain such inaction when it happens in the presence of employees or security personnel, as this may mean that such acts gain legitimacy, to the indignation of the user who does meet its obligations. It can be a source for social cohesion breakage regarding the social value of public transportation.

Instead, with organized groups either to commit massive fraud or concentrations with non-vindictive purposes, the effect on the sense of security, and therefore in the public alarm, is much higher and therefore deserves another treatment by the railway operator. Similarly, induction to fraud and cheating / forgery of tickets with either vindictive mood, for profit, or an increase of social alarm, mainly due to its antisocial character, are a direct attack to system credibility, in particular the tariff system and the control that is expected regarding it.

As for the last column, the level of tolerance of individual and/or multi offender fraud is established by the rail operator in 60.000 fraudulent validations per million, representing 6% of the total. This percentage refers to the frauds detected daily, which occur approximately, and is calculated by counting random empirical different stations in different time slots, both by own staff and by subcontractors.

Table 17. Economic and social impact of incidents for scenario B

Typology	Economic Impact	Social Impact
Individual	LOW	LOW
Multiple offender	MED	LOW
Collective and organized	HIGH	HIGH
Inductive	LOW	HIGH

Scam / counterfeiting for profit	HIGH	NONE
Scam / counterfeiting for vindictive purpose	HIGH	HIGH

In relation to Table 17, far from fraud, the greatest economic impact on tariff revenues are scams and fakes of tickets. Because of this, the profit from the sale of tickets decreases, although they remain equally valid for travel and -depending on the quality of cloning / counterfeit and the security measures implemented in tickets and in the ticketing system- possibly undetectable.

In terms of social impacts, as well as in the other scenarios, it is more visible affected by the subgroups that have protest intent, whether collective and organized fraud, induction and / or forgery and fraud for vindictive purposes. This is aided, no doubt, by performing a communication effort that aims to provide greater transparency and justification by the apparent need of their actions.

Table 18. Administrative and criminal regulation of incidents for scenario B

Typology	Administrative Regulation	Criminal Regulation
Individual	YES	NO
Multiple offender	YES	NO
Collective and organized	YES	NO
Inductive	NO	NO
Scam / counterfeiting for profit	NO	YES
Scam / counterfeiting for vindictive purpose	NO	YES

Table 18 shows which are the current regulations affecting the incidents in this scenario, It should be noted that for the Inductive typology there is not currently any administrative or criminal regulation, as this new type is taking advantage of this No Man’s Land to promote fraud. However, individual who commit fraud because of this may be punished under the administrative regulation.

As regard security measures, in this case, they are of several types due to differences in cases subsets and other factors. The anti-fraud security measures for individual or multiple offenders raise awareness and seek to pursue those who perform it and consolidate and confirm the behaviour of most users. In this case, Information Campaigns promoting good social behaviours fearing reproaches, avoiding its negative effect on the sense of security (for example through Metro TV). Also, Communication Campaigns can be performed to explain and expose users the amount of yearly fraud and what improvements are not done "because" people who commit fraud. Likewise, even more sensitive, Awareness Campaigns are also needed asking the active collaboration of users to address the phenomenon of fraud, without actually making them accountable, but explaining that their collaboration is crucial and necessary to prevent the proliferation of criminal networks such as those that sell mass fake tickets.

To address individual fraud, but especially for multiple offenders, it is necessary the strategic placement of security guards at those stations where, according to previous studies, there is a higher incidence of fraud. If fraud is very high and the locations are well chosen, the simple avoidance of fraud due to the presence of the security guard can repay the cost of the security guard, thereby becoming an investment in security, along with all those incidents that can be detected, while discouraging fraud.

Furthermore, to address a well-organized massive fraud on the occasion of an event or a protest, the situation is more sensitive and requires a different management approach. The main objective of the fraudster in this case, is not to travel or stop paying, but to appear in the media (specific or general) so his message is spread as much as possible. If rail operator attempts to avoid this fraud with the presence of a large group of security guards, and the involved costs of these security guards, the situation will become completely stressful, and the group will take advantage of that to provoke security guards in order to get a disproportionate share in the media and then use the propaganda technique by the act.

Therefore it is important to adjust the resources allocated to each type of incident in terms of the objectives of the fraudster. Otherwise it may have a multiplying effect, in this case, the speaker effect, that is precisely what the authors intend with collective fraud protest, with all direct and indirect costs. This damages the image of the railway operator and generates a greater motivation among the authors to arrange another event of similar characteristics as it is a good way for the message to reach the media.

On the other hand, for the subgroup of "induced fraud", as discussed above, the rail operator must invest primarily in active communication policies through their own media (Metro TV) and general dissemination through the three types of campaigns presented above, information, communication and awareness campaigns. The goals of these campaigns are to provide arguments to not committing fraud, to encourage user to continue behaving civilly, discourage users who would dare, and counteract the penetration of illegal sales channels of tickets by criminal networks.

For the subgroup related to scams and fakes, in addition to regular information and communication policies on security measures, and publication of cases solved with the arrest of the perpetrators of the fraud and forgeries in the press, the most effective security measures are those related to material control and storage of ticket coils. Also, the inclusion of security measures in the support and / or the magnetic stripe of the ticket for differentiating counterfeit / cloned titles and hinder any type of forgery. Furthermore, it is mandatory to explain and train the entire group of Ticket Inspector and security guards on any new security measure introduced in order to detect and filter out any signs of forgery, communicating to their respective structures, together with the security forces, in order to initiate a police investigation to reach users, distributors and manufacturers of tickets.

3. Scenario C: Graffiti.

Usually, the graffiti typology is framed within what is generally known as vandalism, and therefore it has been chosen as its greatest exponent, both because of its economic impact and the amount of resources devoted to its management.

Historically, the existence of the graffiti has been inherent in any railway environment, especially suburban, but in recent years it is evolving in a very unfavourable way, greatly hindering the work of the operators. Currently, the most common perpetrators of graffiti are organized in groups, they have technical and operational means, and use some techniques and procedures similar to other criminals to achieve their goals. The final aim of those perpetrators is not only to vandalize a train, but also, to exhibit, distribute and expose it on the Internet and social networks as well as in ad hoc contests.

The current profile of such graffiti writers is not that of young unemployed people without economic resources, but they are educated and working adults that devote economic resources to graffiti activities that operate in an organised manner, many of them operating transnationally.

There are large differences between those graffiti painters that paint shop shutters, exterior walls or any surface on the streets, and those devoted to paint in railway environment. They belong to different groups, which usually are specialized in one field or the other. Even so, with the today's legislation, where the Collective and organized graffiti painters and the graffiti painters who act with passengers on-board, can be criminal prosecuted, TMB considers that Graffiti painters of the railway environment in general should be classified as more harmful, and this should be reflected both in the legislation as well as in the procedures for judicial and police investigation, for several reasons:

1. Exposure to personal risks for transiting in track areas potentially dangerous for run overs, falls, electric shock, etc.
2. Exposing metro users who travel on trains to risks, as sometimes those are vandalized with users inside and suffer the consequences of sudden braking of trains when graffiti painters cross the tack area.
3. Increased cost of cleaning painted trains, and alteration of the maintenance plans in order to meet the cleaning tasks.
4. Increased frequency of repainting trains, as the original paint is affected by the cleaning products used. This work is costly not only in economic terms but also in time and complexity, as it affects many existing elements and technical systems on board.
5. Environmental impact due to the cleaning products used, besides to the paint used in graffiti.
6. Cost increase of safety human resources.
7. Increase of investment in detection technology for early warning (point and volumetric detectors, motion detection cameras, infrared barriers, etc..)
8. Risks for security guards operating in these incidents, both accidental by having to enter track area, and by the increasingly frequent attacks on security guards who stop graffiti painters red-handed, violently resisting arrest.

9. Impact on the train operations and therefore in the wait time (frequency), so that there is a decrease in the quality of service offered by the operator.
10. Increase of complexity in procedures to access track area, in response to intentional factors, such as withdrawal of trains, passenger evacuation from vandalized trains, train cleaning, preventive presence of security guards in high risk areas or hot spots, etc.
11. Increase of thefts and robberies of keys and access cards in metro facilities to both employees and external staff.
12. Increase of damages of accesses: doors, gates, windows and even on other parts to get access to premises where trains are parked.
13. Rise of management and processing costs in the criminal and administrative areas, to ensure legal defence of the public interest provided to society.

According to current countermeasures applied in Barcelona Metro, any graffiti painted train is removed immediately from service. This countermeasure is based on the application of the “Broken Windows Theory” [17], to avoid promotion / dissemination of their “works” that graffiti painters look for, preventing users traveling on a painted train. According to this criminological theory, any damage or disruption of the normal established order that is not corrected nimbly and persistently, whether uncivic, antisocial and / or criminal behaviour; or by apparent lack of maintenance, cleaning, lighting, information, etc., affects the sense of security, creating greater insecurity among users. This situation increases the possibility of social contagion of these facts, since those who are prone to do, perceiving the disorder and lack of control and performance of the institutions, will be more comfortable to carry out their actions with aspirations of remaining in the anonymity, or at least, becoming unpunished facts.

Therefore, any graffiti painted train is quickly removed from service in order to be cleaned, since it is considered that it contributes to improve the perception of a controlled and maintained, and therefore, safer environment. The benefits are clear, both in psychological and sociological terms for users, as well as in economic terms for the operating company.

In order to see better how to deal with this problem, we have to distinguish the peculiarities and characteristics of different types of graffiti currently detected.

A first classification, from the perspective of those who perform them, we would talk about graffiti of individual or collective authorship.

Technically, graffiti differ by their complexity and number of colours used, and so the most common are made with a single colour and are of small/medium size, commonly called “Graffiti” or “signatures”. By contrast, multi-coloured graffiti, more elaborated, with a primer and better finishes, in addition to being of a larger scale, are called “Wall Graffiti”. The graffiti or signatures are done in any location and their authors are usually not professionals of graffiti and, indeed, as they are performed anywhere, train or location, they are complex to avoid or prevent. Instead Wall Graffiti are performed only on parked trains, and by a group of graffiti artists, which are devoted to it in a more professional and organized way.

Table 19 shows that, at the descriptive level, individual graffiti (it does not affect substantially the company, either quantitatively or qualitatively) can be differentiated from Wall Graffiti, currently one of the incidents that most affect rail operators in every way. Therefore, the low level of organization and typically more spontaneous, single graffiti is more associated with uncivic category. Instead, the three remaining subgroups ("individual multiple offender", the "collective and organized" and "with passengers on-board") are catalogued with antisocial character because of a premeditated and organized manner and with advanced techniques get unauthorized access to premises protected with security systems with the intention of vandalizing trains, taking risks to their physical integrity and the possibility of being intercepted and identified by security personnel and police.

Table 19. Classification of typology of incidents for scenario C

Incident	Typology	Uncivic	Antisocial	Criminal
Indicators of Graffiti	Individual	YES	-	-
	Multiple offender	-	YES	YES
	Collective and organized	-	YES	YES
	With passengers on-board	-	YES	YES



Figure 8. Example of individual graffiti (source TMB)



Figure 9. Example 1 of wall graffiti on trains (source TMB)



Figure 10. Example 2 of wall graffiti on trains (source TMB)

Regarding the perception of users, the following levels of impact in Table 20, are ascribed to the graffiti category:

Table 20. Classification of the effects on the security of incidents for scenario C

Typology	Insecure feeling Allocation	Objective Security Allocation (0-4)	Social Alarm Allocation (0-4)	Tolerance level in number of incident per 1.000.000 users (1 day)
Individual	LOW	2	1	20
Multiple offender	LOW	3	2	10
Collective and organized	LOW	3	3	0.5
With passengers on-board	HIGH	3	4	0.03

With respect to the sense of security, the first three subgroups usually cause a slight feeling of disorder of low impact, unless that their frequency is high and in areas of high visibility and affluence. In this case they affect directly the user perception. If graffiti occurs on crossing points or in inaccessible places they have a minor impact (stairs walls, quiet corners ...), but if it occurs in places where the passage remains for a longer time (platforms or inside trains), the degree of impact on the safety perception is greater.

In contrast, the subgroup that most affects the sense of security is when graffiti painters activate the train stop alarm when the train remains on the platform with passengers on board. By counter-surveillance and their own telecommunications, the authors ensure that there are no security guards on board the train or at the station where they are going to make wall graffiti.

While they make it, they record videos and take pictures and, if they do not have enough time to complete it, as the authors know that Barcelona Metro quickly remove painted trains to be cleaned, they take pictures at other stations before reaching the cleaning facilities.

Regarding objective security, impact, as shown in Table 20 is very similar, impacting all types in a medium-high degree to security, based on the point of view of the rail operator. Likewise it happens with the impact on the social alarm, especially in a context of budgetary adjustments and economic and social crisis, as the resources devoted to fighting graffiti, as well as the cleaning of trains, could be devoted to other more profitable or justifiable targets.

Based on that criterion, the tolerance level of the rail operator, in the case of Barcelona Metro, is a Wall Graffiti every other day, be of concern when this number is increased. In these cases, the operator must perform static and / or dynamic operatives to try to deter or pursue the presence of graffiti in the vicinity of the premises where trains are parked, trying to reach more tolerable numbers.

Table 21. Economic and social impact of incidents for scenario C

Typology	Economic Impact	Social Impact
Individual	LOW	NONE
Multiple offender	MED	NONE
Collective and organized	HIGH	NONE
With passengers on-board	HIGH	HIGH

In line with what has been said, and indicated in Table 21, the economic impact to the rail operator is very high, both for the costs of cleaning and maintenance of trains and facilities (doors, windows, grilles) and the vandalization of detection devices and surveillance cameras, excluding the investments in security resources (human, technical and procedural) required to tackle the phenomenon of graffiti. Moreover, in the last year 2012, there has been a surge of Graffiti activity both quantitatively and qualitatively, graffiti painters becoming more aggressive against Metro own staff and subcontractors, whether or not security staff, engaging in theft and robbery with violence and intimidation, as well as threats and attacks towards employees and security personnel.

For the moment the social impact is not as high as it should be, but it should not be an obstacle to possible legislative changes in the line to distinguish graffiti on roads (blinds, walls, etc.) from graffiti in the railway environment (on trains), because of its unmistakable charge of social contempt towards a public service and its greater impact on public budgets. In this regard, we must not forget that those who suffer most the consequences of a poor transport network are the users, that often fit the profile of a citizen who does not have easy access to other transportation alternatives, and not only for economic reasons, but also social (age, entitlement to drive, presence of disabilities, etc.).

Through information and communication campaigns, led by the railway operator, it is possible to increase the general awareness of both users and policy makers, as long as regulation about the phenomenon will allow a more effective management, but also more efficient in terms of economic and resource optimization.

Table 22. Administrative and criminal regulation of incidents for scenario C

Typology	Administrative Regulation	Criminal Regulation
Individual	YES	NO
Multiple offender	YES	YES
Collective and organized	YES	YES
With passengers on-board	YES	YES

Table 22 reports the regulations affecting the different types of graffiti. Following an amendment to the Spanish criminal law in December 2010, graffiti that were considered a crime of damage (art.263 CP: Whoever causes property damage not covered under other titles of this Code, shall be punished with fine of six to 24 months, attended the economic condition of the victim and the extent of injury, if it exceeds 400 euros) were

reduced, being considered criminal lack of property (Art. 626 CP: Those who spoil movable or immovable property of public or private, without permission of the administration or their owners, will be punished with the penalty of permanent location from two to six days or to three to nine days of work for the benefit of the community): it is no longer a crime and not valuable in the courts and therefore by the police.

This modification makes it difficult to act effectively against this phenomenon of vandalism in the courts, winning a crucial role administrative complaints for infringements to travellers regulation, which depends only on the rail operator and related authorities (the Directorate General of Transport and mobility, of the Catalonia Government, in the case of Barcelona) who has the authority not only to punish such conducts, but to do so in a progressive and proportionate way according to the circumstances and effects of each case.

So to avoid the judicial costs, both in actions prior to the criminal complaint and also during the judgment, and other internal costs, it is only recommended to prosecute in those incidents in which there is evidence on the authorship of graffiti, either because the author has been identified in the act or because there are identifying video recordings available. In case of identifying any graffiti painter committing an infringement to travellers' regulation, with the intention of deterring his behaviour for future occasions, in addition to the courts, it is proposed to the Administration to impose all those administrative complaints based on observable behaviour that has carried out at Metro facilities.

4. Scenario D: Pickpockets.

The phenomenon of pickpockets is also a recurring problem in rail transport, with different quantitative and qualitative intensity, and, as noted before, it is a concern in many subways worldwide.

In the case of Barcelona, it is a problem inherent to the city, since many variables influence the phenomenon:

1. Criminal and procedural regulation is more rights-based in Spain than in other countries of southern Europe.
2. The application of existing regulation is not entirely effective in the courts, either by saturation of cases or by lack of financial, technical and human resources. Also, the chances of judicial success can become difficult because of slow reaction time, especially when victims are tourists and they have to make a criminal complaint and a quick trial (or at least to testify) before returning to their country, prerequisite for condemning the identified pickpocket.
3. The city of Barcelona is a touristic destination. This fact provides having in a reduced space tourist in an unfamiliar environment, often carrying large amounts of money with them, with a high purchasing power showed in high-end segment mobile devices and digital and video cameras. In the same environment, there are found opportunistic criminals, who know perfectly the spatial, legal and police context, taking advantage of the situation so they can steal the belongings of tourists and / or locals in misplaced attitude.

Table 23. Classification of typology of incidents for scenario D

Incident	Typology	Uncivic	Antisocial	Criminal
Indicators of Pickpockets	Pickpockets announcements	YES	-	-
	Thefts due to carelessness	-	-	YES
	Thefts by organized groups	-	YES	YES

In relation to this type of incident, in TMB it is internally divided into three subgroups, as can be seen in Table 23, depending on their sociological typology, economic and social impact, and what of management is required within the rail operator's decision scope.

The subgroup of Pickpockets announcements is considered merely uncivic because it notes the presence at the station and/or trains of people that normally had been identified as pickpockets. These people spend whole days wandering the premises in search of their opportunity for theft and being often detected by customers, security guards or police officers in uniform. They automatically leave the station, re-entering again after a while or by another location where they believe they will be more relaxed in order to perform their criminal activity. Against this, as operator, little can be done more than invite them to go out (always according to their free will) given that that day they may not be "working" but simply have chosen to use public transport as a user, a fact that as Rail Operator cannot legally prevent. Therefore, administrative or complaints cannot be applied. Even so, if they are detected bothering the passengers or employees (committing fraud, being near the passengers, holding the train doors, wilfully obstructing the normal flow of people to organize tumults, stopping the escalators, fighting each other, discussing and / or insulting users and / or employees that warn them, etc.) an administrative complaint is imposed as stipulated by the regulations, not because they are pickpockets, but for the commission of an unlawful conduct at the administrative level.

Table 24. Administrative and criminal regulation of incidents for scenario D

Typology	Administrative Regulation	Criminal Regulation
Pickpockets announcements	NO	NO
Thefts due to carelessness	NO	YES
Thefts by organized groups	NO	YES

Table 24 reports the regulations affecting the different types of pickpockets. Depending on the profile of the pickpocket and its economic and legal residence status, the administrative complaint can be more or less deterrent, but in any case, the fact of being stopped by security guards, and then, waiting for Mossos d'Esquadra (Police) to be taken to police station to be identified properly, etc, makes this all a waste of time in which they could be "working" in the Metro.

On the other hand, if their behaviour goes beyond faulty at administrative level, it becomes a typified criminal conduct, such as insults, humiliation, slander, assault, attempted robbery or theft, which are reported by criminal proceedings, as well as

administrative complaints when they are justifiable on the basis of conduct carried out within the Metro premises.

Another subgroup is theft due to carelessness and it refers to all those events in which we detect the existence of a victim of theft, either because it communicates via SOS intercom or through security staff. Like the other subgroups, there is in this case also a bias since there is no capability to detect all those events that occur in the underground facility, and are reported, or those that are not, but are known based on victimization surveys. In any case, its shift over time is another indicator of the evolution of this trend that allows comparison of the level of crime detected by the operator at any given time. This typology corresponds to a criminal who works isolated and on an individual basis, that is not engaged to it in a systematic way, but when detects an opportunity he does.

Finally, the subgroup of "Theft by organized groups" is considered a relevant type, with a different social impact. They are groups between three and ten organized pickpockets, disguised as middle or high class citizens / tourists to be unnoticed and performing throughout the day and in a professional manner all the thefts that can not only opportunistic but creating those appropriate situations (some with some violence and soft intimidation) enabling them to increase profits, while acting with greater impunity and increasing the risk of being held when detected by the passage and / or by employees or security personnel. This subgroup, for internal and legal purposes, is considered criminal. But recently this behaviour can be considered as antisocial too, because it is getting worst causing and acting with clear disdain against victims and witnesses that detect them before or while performing this criminal actions.

According to the type of behaviour taken against employees or security guards, if a criminal complaint is made and if the offense falls into the section of the Criminal Code "Crimes against persons", i.e., insults, threats, injuries, etc. the prosecutor and the judge that try the cause may considered, in addition to the sentence associated with the offense, a restraining order to public transport for a specified time. This measure, very novel in Barcelona [18], is well-grounded in the fact that the work of the victim is performed in rail transport facilities, so as long as there are transportation alternatives for the pickpocket, a judicial measure like this can be imposed preventing him from using the rail transport. If the pickpocket fails to comply with this injunction, this would mean a crime of breaking sentence, punished with imprisonment.

Likewise, if instead of being a crime against persons, it were a crime against property, the police can demonstrate that it is a usual pickpocket or multiple offender, demonstrating his authorship in four or more not judged facts, he also be liable to a restraining order by a certain time, forcing pickpocket to move to other transport, regions or countries to keep on doing the same activity.

Table 25. Classification of the effects on the security of incidents for scenario D

Typology	Insecure feeling Allocation	Objective Security Allocation (0-4)	Social Alarm Allocation (0-4)	Tolerance level in number of incident per 1.000.000 users (1 day) ⁶
Pickpockets announcements	HIGH	0	3	20
Thefts due to carelessness	MED	3	4	2
Thefts by organized groups	HIGH	4	4	2

Regarding the effects associated with this phenomenon, as described in Table 25, it increases as the more explicit and obvious is the fact for transport users. The mere presence of pickpockets (warning pickpockets) has a high impact, since the notice is issued due of a high probability of committing a criminal act. In the same way, collective and organized theft generates a high level of insecurity and helplessness which favours optimal conditions for committing the crime.

Nevertheless, we must bear in mind that it is a criminal typology seeking anonymity per se since they are opportunistic and occasional facts and seeking the occasional carelessness of the victim. Usually, the victim becomes aware of the theft outside the facilities, when he misses his wallet or mobile phone, fact that, depending on the case may be related to the last Metro ride or outdoors. This makes the subjective feeling of security largely dependent on how detectable the incidents are and if one speaks or not about it in the media. Unlike the other types outlined in the three scenarios previously described, this type usually is not seen nor appreciated by users, only by those who are observers and by the victims themselves.

The number of occurrences of pickpockets warnings depends on the number of human resources available in the network, since more staff is distributed, more incidents are detected, which does not necessarily mean that the security status or perception of safety is better or worse or has been altered, but merely more cases are detected and reported. So it should be taken into account the schedules of the security personnel or employee in each period (in case they change) to include a correction to the statistics before undergoing to analysis. In particular reliable conclusions can be drawn when it comes to sudden increases or decreases in this indicator in periods when the availability and utilization of human resources throughout the Metro network is stable and the presence of this issue in the media is not altered.

Also, to fight this phenomenon, the public transport operator can perform different actions beyond the war of attrition that supposes to detect and evict them from Metro facilities whenever they are identified. Some examples of these actions are:

- Through information and communication campaigns, either through permanent messages through the PA system in trains and stations, especially in those stations frequently visited by tourists.

⁶ These includes only incidents detected by the operator

- By increasing the frequency of trains or improving spaces so that users do not bunch up and can be distributed more evenly through the stations and / or trains (to reduce the overcrowding).
- Through the on-going dissemination of awareness instructional videos on how pickpockets act, giving clear, direct and concise advices to potential victims.
- Through deterrence by the presence of employees and security guards in hot spots of the Metro network, etc.

Videos are broadcasted continuously, with particular intensity during the touristic seasons, or when the indicators of incident rise to unacceptable thresholds. As well as in times when social stress detected on users' complaints or media is very high. Several videos, more or less explicit, have been broadcasted progressively to avoid creating social alarm among users. This same technique of using video communication campaigns has been used with other types of incidents, such as with found and suspicious objects to prevent terrorist attacks, also progressively and intermittently depending on the alert level of each moment.

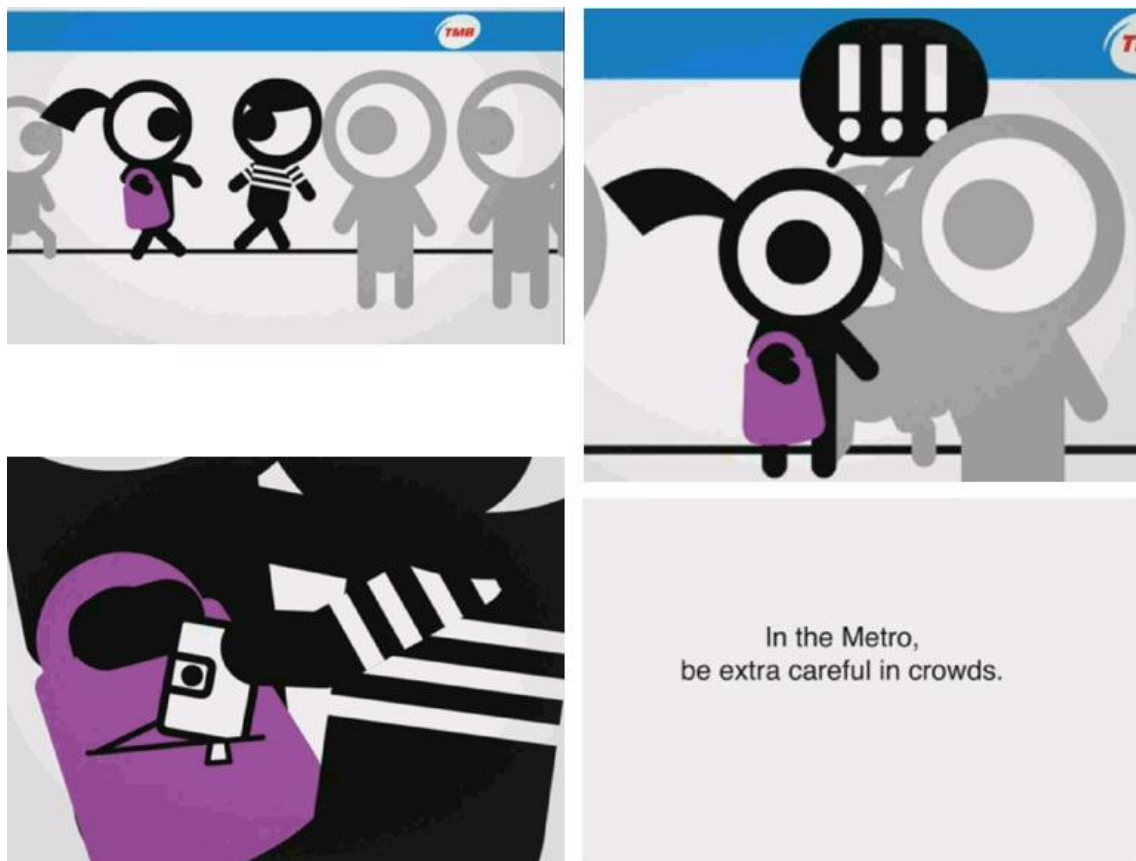


Figure 11. Samples of videos broadcasted through Metro TV (source TMB)

Another example of what an operator can do is related to the "recovery of found objects," referred to the recovery of all those abandoned objects that come from thefts or robberies, such as handbags, wallets, purses, bags or suitcases. This indicator, despite its manifest bias, gives us a rough index of the level of criminal activity in relation to theft, in the absence of official data on complaints brought to the security and police

forces, which would be less biased and more specific information. Despite its bias, this information complements the incidences of "Notices of pickpockets", as both types should statistically be up and down in parallel, as they are indicators directly related to these activities.

Also, as a later step, not preventive, bearing in mind the impact on a tourist that has been robbed during his holidays in a foreign country and requiring his documents and belongings to return to his country of origin, Barcelona Metro coordinates with the police, and in some specific or urgent cases with Consulates to contact the victims and provide them, the fastest possible, their belongings that have been found, so as to reduce their discomfort as the incident happened inside the operator's premises. This is not to forget the importance of watching over and protecting the victims of these crimes that occur quite often. Being this one of the few things that can be done for the victims, it is often treated as something not essential or with low priority.

With regard to the rail operator economic impact of this type of incident, it is very low: the users who stop using public transport for fear of being stolen are estimated to be a minority. Nevertheless, as shown in Table 26, the social impact of antisocial and criminal typologies is medium to high, especially when the levels of criminal activity of the phenomenon exceed the tolerable and acceptable thresholds at social level and this phenomenon becomes present in the media.

Table 26. Economic and social impact of incidents for scenario D

Typology	Economic Impact	Social Impact
Pickpockets announcements	LOW	LOW
Thefts due to carelessness	LOW	MED
Thefts by organized groups	LOW	HIGH

4.2 Key validation indicators for current threats

The main tool to quickly assess the security situation in the metro network, in a particular line, or even in a particular station, is the *Segurómetro*⁷. It is a TMB basic management tool that describes spatial average of security incidents on a monthly basis, differentiating the issues affecting the sense of security and those that affect the objective security.

The tool allows to compare the safety objective (number of incidents classified as related with safety objective), and the subjective feeling of security (number of incidents classified as related with the subjective feeling of security), and shows the quantitative values of security in general, assigning a colour that allows quickly assess its status.

⁷ Definition can be found in ANNEX 3. Glossary

In the following **Error! Reference source not found.**, the incidents are classified according to their category:

Table 27. Classification of incidents according to the type of security perception

Category	Threat
Objective Security	Acts of Vandalism
	Aggression
	Threats
	Fights
	Drug Consumption in Public Places
	Scam
	Indecent Exposure
	Petty Theft
	Annoyance / Uncivic Behaviour Affecting People
	Painted Graffiti
	Mural Graffiti
	Scratches
	Robbery with Force
	Robbery with Violence and Intimidation
	Illegal Trafficking / Possession of Narcotics
	Breaking or Disabling Metro Components
	Broken Access Door Pair
	Broken Glass of Fire Extinguisher Cabinet
	To Find Items of Special Care
	Domestic Violence
Subjective feeling of security	Uncontrolled Access of Street Peddlers
	Musicians Detection
	Tramp Detection
	Arson
	Warning of Pickpockets
	Uncivic Behaviour of a Sexual Nature
	Alcohol or Other Drugs Consumption
	Handing Out Flyers or any Other Type Advertising
	Enter in Tracks Area
	Sleepers Detection
	Smoking on Trains or in Facilities
	Improper Operation of Underground Material
	Open Stations' Emergency Doors
	Hazardous or Annoying Materials
	Unauthorized Presence of Animals
	Doing Bodily Functions
	Remain in Facilities Out of Opening Hours
	Misuse of Alarm Appliances
	Generic Hawkers
	Travel with Unauthorized Items

Category	Threat
	Travelling in Inappropriate Places
	Travelling Without Transport Ticket

Error! Reference source not found. describe the three colour codes representing the three different stages of security status:

Table 28. Colour classification for security status

Status Colour	Description
Green	High security level, not requiring special attention
Yellow	Security level that requires specific attention
Red	Security level concern. Requires specific and fast treatment.

The bounds between the values green-yellow and red-yellow are dynamically calculated based on the number of detected incidents and the number of stations. The formulas for calculating these border values are presented in **Error! Reference source not found.**:

Average number of incidents = Total number of Incidents / Total number of Stations

Table 29. Formulas for bounds calculation of security status

Bounds	Description
Green-Yellow	Average # of incidents
Yellow-Red	5*(Average # of incidents)/3

4.3 Effectiveness of security measures

This is how countermeasures detailed in section 2.1.4 are applied according to the scenarios described above.

The optimal allocation of resources and their effectiveness for each scenario is based on the experience gained by TMB, and the observation of the effects on the application of the security measures on each type of incidents. Some resources does not have a direct impact on the decrease of security incidents, but in the passenger's subjective feeling of security, as it is the case of the SOS intercom totems, CCTV or PA systems. The tools used for the measurement of the impact of the security measures are a) "Segurómetro", detailed in section 2.2, which provides a measurement of the evolution of the subjective feeling of security and also of the objective security, and b) the surveys performed every year by TMB, which, among others parameters, provide a measurement of the passenger's feeling of security.



Figure 12. Security staff in platforms (source TMB)

1. Human resources:

They are primarily oriented towards uncivic behaviour and early detection and reaction to antisocial & criminal behaviour.

All the human resources, without exception, have a deterrent function that, depending on the case and type of incidents, manage to avoid them or, in its absence, deviate them from uncivic, antisocial, or criminal behaviour. For example, the case of ticket inspectors: they are primarily in charge of tickets control, but that does not mean they cannot warn of any unlawful conduct, thus becoming potential "whistle-blowers" for any type of incident.

Regarding the preventive level, it is directly related with the distribution and amount of resources arranged across the Metro network, located according to preventive parameters mainly.



Figure 13. Security staff in hallways (source TMB)

In the reactive level, the role of every resource is different. The ticket inspectors, as employees, are limited by procedure to warn the presence or detection of an unlawful or criminal conduct, as long as they can communicate safely to their physical integrity. On the other hand, for the remaining staff, which belongs to the external private security staff, the expectation is much higher because, in most cases, they should also try to identify the person who has committed the unlawful or criminal act, based on their role of law enforcement agents and the procedures and legal limits. In any case, the measures

used should be proportional to the severity of the situation.

In the case of the sniffer dogs in the reactive level, besides deterring as security dogs do, their job is to detect explosives in abandoned or suspicious objects.



Figure 14. Security dog (source TMB)



Figure 15. Sniffer dog (source TMB)

2. Procedural resources:

With respect to procedural resources, they can also be flexibly used.

SOS calls that any user or employee can perform through the SOS intercom totems, are used for any communication involving a security incident. Still, rather than a decrease of objective security incidents, its mere presence influences the user's security perception, both of those who have exemplary behaviour and those who occasionally have an unlawful and / or criminal conduct. The fact that the security perception increases, not only affects positively the user, which will feel more secure, but also affects the uncivic, antisocial and / or criminal because they feel less unpunished and therefore certain percentage of antisocial, antisocial and / or criminals shall decide not to act, especially the opportunists. It is the same case as for some technical resources described below, as is the case of the permanent presence of CCTV in all facilities with permanent video recording.

Understandably, the permanent checking of tickets by ticket inspectors tries to be:

- a) a dissuasive measure for all those that attempt to commit fraud and not validate their ticket,
- b) a reactive measure for all those who finally do it and
- c) an enforcement measure and justification for those who decide to correctly validate their tickets.

Regarding the administrative complaints, whether inflicted by an employee or by security staff, their aim is to punish those "uncivic conducts" and "moderated antisocial conducts", given that the "non-moderated antisocial conducts" and the criminal acts are persecuted through criminal procedure. This punishment intends the person to reconsider their behaviour, and that he won't do it again, whether through convincement or by fear of receiving a criminal complaint. Thus, the imposition of administrative complaints is a reactive counter measure that helps to prevent, avoid or diminish future uncivic and "moderate antisocial" acts, like in the case of fraud, accessing tracks area, disturbing the passage, soiling facilities, etc. The facts that are not reported administratively are mainly damage to facilities worth more than 400 € as well as those which are qualitative considered serious, whether motivated by recidivism or any other severity criterion.

3. Technical Resources:

As just stated, the video surveillance cameras, both located in stations and on board of trains, rather than seeking a direct decrease of objective security acts (criminal and antisocial not moderated), they aim to increase the security perception, as well as to clarify the facts afterwards with the video recording.

By their mere presence, these resources influence user's security perception, both of those who have exemplary behaviour and those who occasionally have an unlawful and / or criminal conduct. As mentioned previously, the fact that security perception increases, not only affects positively the user, which will feel more secure, but also affects the uncivic, antisocial and / or criminal because they feel less unpunished and

therefore certain percentage of antisocial, antisocial and / or criminals shall decide not to act, especially opportunists.

Other technical resources which are very useful and are permanently used, are those information media (PA systems, station and train televisions, informative panels and communication through social networks) that allow communication with the user, at any time, either as a preventative measure, alerting different risks (e.g., pickpockets) or reactive (specific incidents affecting Metro service). As long as the users are informed, get quick answers to their questions and uncertainty and therefore, they can redirect their discomfort, for non-compliance of the service, toward an external cause not related to the organization, maintenance or management of the Metro service.

This resource is especially used preventively to avoid risks of pickpockets and /or implement sensitizing behaviours on fraud, crossing track areas or smoking in the facilities. Likewise, it can be used reactively in those security and civil protection incidents affecting circulation and, therefore, the Metro service, such as intrusions and vandalism by the graffiti collective.

5. Urban transport scenarios based on emerging threats

The event logging system used at the Security and Civil Protection Centre is very dynamic and it easily allows creating descriptions of new types of incidents. So, once detected a new type of incident, the head of the Centre of Security and Civil Protection creates the new category in the database and begins monitoring its evolution since then.

In all cases, at the time of identifying a new type of incident and registering it in the database, it begins to monitor its progress. There are some specific types of incidents that only happen once, or happen again in a very sporadic way. The incidents that clearly show an increasing trend are prioritized and proper measures are defined to prevent and/or to face them. The evolution is measured both quantitatively (frequency, concentration on schedule / calendar) and qualitative (degree of impact / severity on people and service).

Given a high degree of quantitative affectation, and working with situational prevention parameters, the circumstances that make possible the occurrence of considered incidents are avoided. The physical and human environment affected requires greater monitoring and feedback information to ensure the on-going adaptation of measures against possible changes in the situation.

In the case of incidents with high impact, the situation is dealt in an extraordinary way with the company Management and/or with the city security forces, to address the incident and to identify the specific measures to prevent and/or to face them. In such situations, it is vital to design a service plan long enough to avoid new shoots that are not treated and addressed swiftly, and in addition, a communication plan that ensures sufficient transparency and restore the credibility of the citizen in the technical reliability and security of the service.

In regular meetings with the city security forces, impressions are exchanged about the incidents as the security incidents given in the subway are only a reflection of what happens on the surface. These exchanges allow tackling incidents quickly and efficiently. Nevertheless, we should point out the benefit of having a transport police, specialized in the investigation of incidents, both criminal and incidental. Specifications and complexity of police actions in transport networks are greatly benefited by this specialized approach.

The value of this tool, especially based on the comparison of results over different periods of time, either on a monthly, quarterly, biannual or annual basis, is that it can draw conclusions about the trend and pattern of the number of events detected in each facility, so that helps to adjust the technical, human and procedural resources to the amount of detected events, even assuming that it is a tool with a high bias during the information collection phase, failing to detect all events occurring in different units and/or trains of the Metro network.

5.1 Description of scenarios

As already mentioned, the assessment or better judgement that the citizen makes about the security issues is variable, depending on the nature and the level in which it operates.

Following the classification of the previous scenarios, it is appropriate to establish emerging threats in relation to uncivic behaviour, antisocial and criminal acts.

Uncivic behaviours

These are the most common behaviours and attitudes that affect subway service and the customers' safety perception. There are many types of uncivic behaviours occurring on a daily basis, that it is more relevant interpreting the evolution or the degree of citizens' acceptance / rejection towards them, than expecting new types of uncivic behaviour. The economic, social, cultural and environmental factors, among others, play some role in the impact degree of incivility and other environmental factors.

It's important to consider that the change of the sense of insecurity towards some degree of social acceptance is a slow process that badly tolerates the abruptness and force positions. This is true precisely when adverse experiences are individual, rather than promoting social awareness. The opposite is what happens when shocking criminal acts, gain notoriety and seriously affect the subjective feeling of security, although usually such type of events are rare or even extraordinary. In these cases, the degradation processes of the sense of security can happen very fast, although the recovery process also takes place in the same way.

A typical example might be the murder occurred when a passenger pushes someone deliberately toward the tracks when the train enters the platform: it is a singular event (it only happened once in Barcelona underground, with a very similar situation in other metros in the European continent) with a very high impact on citizenship, experiencing a crippling sense of incomprehension, disbelief and restlessness which translates into a fall of the sense of security. Even some changes in the behaviour of passengers may appear, as waiting for the train in the platform next to the wall. Fortunately, after the initial impact, normalcy gradually returns to the daily routine of large cities.

In an environment like this, where there is a particularly unfavourable economic situation, it is likely that individual behaviours promote a rise of fraud, and therefore it is perceived deterioration in living standards and economic sustainability. This is a point shared by all operators worldwide. In these circumstances, the authorities and operators are obliged to do something. This is not the kind of problem that comes to stay with us a short time, quite the opposite. This explains why some networks traditionally without toll lines, are introducing them, both at the entrance and exit, if facilities allow it (e.g. Rotterdam, Netherlands and in Brussels, Belgium).

In the future we may have to forget about solutions based on a single measure, on the contrary, we may need to perform a kind of magic formula, which adjusts the amount of

ingredients (measures) as needed. Some people think that the relationship between strategies and tactics is changing, and probably they need to achieve a flexibility that until now was not imaginable.

The strategy must be established through action plans, which fully cross organizational structures of the operators, and give sense to the different types of actions, information (campaigns), reactive (complaints), and technological (replacement of turnstiles by higher reversible doors, well-protected tickets against counterfeiting or individual misuse). These performance parameters are applied to any type of relevant situation that arises, adjusting the singularities that each case requires.

Anti-social behaviours

A particular case corresponds to anti-social acts. As previously explained, this is characterized by rejection acts towards society and the values system shared by most citizens. Their organizational features, recurrence or intent are important, but the most important is the propaganda that accompanies these activities, a self-justification that reminds the sentence of the ancient Romans: "Excusatio non petita, accusatio manifesta" (explanation not requested, guilt manifests). They need a social impact to the established order, both fighting for ideological reasons (anti-system), or those with an absolute insensitivity to the social consequences of their acts (graffiti).

The convergence of different activities, some clearly characterized as criminal, and others on the edge of becoming criminal, have evolved perfecting their capabilities to run increasingly synchronized and unpredictable actions. If additionally it is considered the potential that new technologies have provided, especially the Internet, it is easy to imagine a future growing trend.

Of particular concern is the increase in violence, particularly in groups close to the anti-system ideologies. This is what happens now with the graffiti: traditionally nonviolent, they now cause assaults and serious damage as usual.

One possible explanation would be the middle ground where antisocial actions are about incivility and criminal actions. Any evolution of both can come together in this middle ground, by necessity or convenience, and that hides the true background of the motivations that drive them and justify their actions.

The most commonly problem shared by all international operators is graffiti on trains. The worst thing is not the number of people who carry out these acts, very small, but the complexity of their actions to counter the lack of understanding of laws that ignore their enormous and destructive effects. Cross-border activities and the use of internet and social networks allow making public their "works" and the information needed to spread this "fashion" or even "art" as some still believe.

Another emerging problem is the proliferation of organizations that attempt to promote fraud practices through various techniques that do not detract from the objective, which is to fight the operation and financing of public transport system. This

organizations make use of virtual platforms, that provide slogans (e.g., MeMetro, they aim the people committing fraud to justify not validating the ticket when entering the metro due to a memory disorder), the exchange of used tickets by people leaving the premises that provide them to other users to use the remaining time to commute to another public transport, or real-time information about the existence of ticket inspection controls.

Worst of all, it's a breeding ground for systematic ticket alteration or counterfeiting, clearly criminal activities. Countermeasures to use must be carefully planned, as they play through mass communication and cross-border activities. We must make a major effort, but necessary, in order to know the nature and objectives of these behaviours. If there is no uniform approach from different government bodies, operators do not have at their disposal an effective way to act.

Communication campaigns are vital, because if the public does not interpret the situation with accurate information, it may get only the information from the authors of these acts. Do not forget that for a misinformed customer it is easier to walk the road that joins dissatisfaction with insecurity.

Criminal actions

Although usually there are not serious events at individual level, as a result of the accumulation of criminal actions can be, without doubt, a bad image and collective consciousness of them can cause a clear deterioration in the perception of security. The most notorious case is the quintessential pickpocketing, scourge of almost all transport operators, especially in cities where tourism is the benchmark.

Another issue with uneven affectation but shared concern is metal theft (mainly copper). As with some of the antisocial acts (e.g., graffiti), cross-border activities are a note of paramount importance. Metals travel to other countries through international criminal networks, and in the case of pickpockets, they are the ones who travel looking for more favourable places to "work". Sometimes even the effects of their crimes give support to counterfeiting networks or funding for other criminal activities.

In this area, operators need more than ever to work closely with the security forces. As usual, keeping a silent attitude to tackle this problem does not generate any good perception in the public, as it is well familiar with the existence and magnitude of the problem. Instead, clear communicative guidelines must be undertaken with complete information, public awareness communication campaigns -as it is more appropriate to inform citizens of complex situations- and lines of action to act proactively.

The arrival of other emerging criminal actions is not expected, except those coming from consolidated antisocial acts (massive fraud, tickets scams...), and the already mentioned and shared activities (e.g., graffiti). It must be remembered that normally the severity of these events is determined by its multi recurrence, so it is vital to reliably determine the acceptable tolerance level, and act accordingly at the tactical

level, without forgetting the importance of necessary diffusion through the mass media.
[19] [20]

5.2 Key validation indicators for emerging threats

As reflected in the previous point, it must be possible to speak openly about problems affecting citizens in a direct and serious way. Lack of transparency is not justified, because nothing related to state security or classified materials is running. We must begin to outmanoeuvre the myth that talking about certain issues leads to insecurity, or even social alarm. This is not a toll, but it is the first step to be able to establish social tolerance levels of impact of uncivic, antisocial or criminal events. Without those concerning objectives, there is no way to choose what level of action and in which areas are the most efficient, and an overreaction is as possible as the opposite.

Once down this road, a challenge in the current situation is involved in most societies, we must ensure a homogeneous study of the evolution of indicators showing improvement or worsening of the situation, that is, the degree of success or otherwise of countermeasures.

In this process, it is very important that operators take an active part in the strategic decision making in this area. It's important to consider that everything happens in a place that performs the function of transporting exclusively (cannot be reconciled with other activities) and exclusive (nature itself makes impossible to be otherwise), and therefore, is intrinsically linked to this activity. Failure to do so is to ignore an interpretation more in line with reality regarding effects and consequences of certain actions that can have on the service and the perception of the users.

It is particularly relevant to bear into account the need to address this issue at the international level, especially in situations where the facts have a cross-border nature, in the origin (metal theft trade) or where it occurred (graffiti).

6. Security framework definition for urban public transport

6.1 Security framework requirements

Security in the subway is closely integrated with the security model of the city. Thus, the laws and procedures applied in case of incidents which affect the subway, are the same of those applied to other incidents in the city, while TMB tries to raise awareness among the stakeholders that the affectations of the service (not referred to explicitly in the law) should be treated with special sensitivity, given their high impact on the users of the system.

Saying that, it is clear that the stakeholders that are involved in these cases are the same as those involved in the incidents in the city.

The security forces (Mossos d'Esquadra, National Police, Civil Guard and local Police of the affected municipalities), courts, fire-fighters and emergency services, neighbourhood associations and councils are directly involved, and the public transport operator works hard to raise awareness and facilitate the actions they should take.

The management of TMB performs actions of closeness and awareness of these stakeholders so that they understand the peculiarities affecting a service like metro and the magnitude of affection towards many users when an incident occurs in particular. TMB also actively participates in specific collective awareness, such as schools, for sensitizing young people of the usefulness of the system and the need to preserve it in the best possible conditions.

The currently most used tool to align objectives with stakeholders is the establishment of bilateral cooperation agreements which discuss the specific needs that must be covered and describe the procedures to be followed for this purpose. For example, in the field of Justice, TMB has signed an agreement that establishes guidelines for action after a run over on tracks, and that, after ensuring the legal procedures are followed, greatly reduces the impact on service time.

A next necessary step to improve joint actions of the stakeholders with the transport operators is to study, jointly, the search for common scenarios in which the administrations should regulate procedures of performance standards with the aim of simplifying the current model and make it more coherent.

Traditionally, one of the weakest points is the relationship with users' associations in relation with subway's security. Despite this, a close collaboration started with some specific collectives such as groups representing people with disabilities or at risk of social exclusion. The model should aim towards fluidity in the relationship with more extensive groups of users such as neighbourhood associations that currently interact with operators though not addressed the specific issue of security.

6.2 Stakeholders perspective for a new security framework in the urban public transport

During the workshop held in the course of the UITP Commission on Security meeting organized in Munich on the 7th and 8th of November 2012, a specific survey was submitted to attendants. Detail about the meeting, the questionnaire and the answers can be found in section 3 Stakeholders & Engagement Plan and also in *ANNEX 2. Internal validation*.

A total of 6 questionnaires answers were collected among 22 attendees to the specific workshop. So the return rate was 27%. The questionnaire focused on the following topics: Security decision-making, Data requirements and evaluation of security measures, Strategic requirements and Tool requirements.

All questions except the first one, were presented in a multiple answer choice, and a rating of priority of selections was required: 1- top priority; 2, 3, ... - less priority.

The tools requirements group of answers is complimentary with the information provided in section 10 of D3.2. As well, the other answers are related with the process of decision making regarding security issues, the relation with different stakeholders, and the strategic requirements regarding regulations.

The questionnaire was developed on the base on the work developed in the Valuesec project, regarding the factors influencing security-related decision-making [21].

Conclusions from the answer are as follows:

I - Security decision-making

Regarding the approach towards security, 66% of respondents confirmed that they have a strategic approach instead of an operational approach. That means that most of the public transport operators try to address the causes of the security threats (proactive) rather than addressing the symptoms (reactive).

About the priorities when addressing security-related decisions, top rated answers are, by this order, passenger's real security; facilities security; passenger's security perception. This means the security of people and facilities are the top priorities. In fact facilities security, besides providing security to the assets, also results in providing security towards users, as it keeps integrity of equipment which is vital for providing a secure and reliable transport service.

In question 3, about stakeholders influence in the security decision-making process, top rated answers are: local, regional or state politicians (parliament members, mayors); organization personnel; citizens. The answers to this question reflect what is already in the EC legislation, Railway Safety Directive [14], which recognizes that metros, trams and other light rail systems are subject to local or regional safety rules, and supervised by regional authorities. After local authorities, own transport organization personnel and citizens are the main stakeholders in the security decision-making process.

About the main societal impacts taken into account in the security decision-making process for the transport operators, the top rated answers correspond to, internal acceptability / company policies; legal; public safety. So, internal policies are the main issue taken into account when making security-related decisions, probably to keep the integrity of the security policies. Otherwise a failure to do so could cause some confusion for users. If any important change affecting security policies must be introduced it should be done gradually.

When it comes to the biggest challenges facing public transport organizations, top rated are, availability of data; process, influence of different stakeholders and different perspectives of the security problem. Then getting available all the information about the security threat and the different perspectives stakeholders may have about, it is the main concern of decision-makers.

Regarding dependencies that have some degree of influence over the decision-making process, the top ranked answer is the own organization internal procedures, followed by some other external dependencies, like political and economic environment, information available and regulations.

II - Data requirements and evaluation of security measures

About the method employed to calculate the cost and benefit of new security measures, qualitative analysis is the most widely used method, taking into account what the costs of not deploying such measures would be. This is also complemented with the assessment of quantitative tools.

III - Strategic requirements

About the question if some security aspects should require some regulation, probably at European Union level, to improve security in public transport, the most supported answer is to establish some minimum security measures according to passenger volume, followed by a standard passenger regulation.

IV - Tool requirements

Requirements about tools for supporting the decision-making process, usability, flexibility and interoperability are the most important ones, as they allow: ease of use, tailor the tool to the requirements of each operator and the integration with other existing tools and databases. The factors mainly valued if a tool should be able to report are, the prioritisation of security measures and the effects each measure can help to avoid.

7. Research questions

As it is described in section 2.1.3, **subjective feeling of security** may require research in order to provide a wider perspective on the environmental and ambient factors influencing such perception on users, beyond the known factors listed in the previous section, and the proper way to address them from the operator’s point of view in an effective and efficient way. This question should be addressed by technical WP4 which deals with the people and society aspects of security.

Technical WPs, i.e. WP4, WP5 and WP6 suggested some relevant research questions to be analysed during their modelling activities.

In WP4, ISAS CR proposes to develop a model based on the effects of various security measures on costs/benefits and customer satisfaction as detailed in Table 30.

Table 30. Model based on the effects of security measures

Type of security measure		Cost		Profit		Effect on customer Satisfaction/ Level of acceptance
		short-term	long-term	short-term	long-term	
Duration		short-term	long-term	short-term	long-term	n/a
Human resources	Single guard	high	medium	low	low	rather negative/low
	Guard with dog	high	medium	medium	medium	negative/low
Technical resources	CCTV cameras	high	low	medium/high	high	neutral/high
	Turnstiles	high	low	high	high	negative/low

This model could be enhanced to include other measures, and tested based on TMB data.

Following there is a description of quantification levels. The categories are not mutually exclusive, but cumulative.

I. Costs

I.1. Human Resources Costs

Values: high - medium

High: personnel recruitment, personnel initial training (taking into consideration personnel turnover), additional/specific training (e.g. in connection with new technologies). This has to be included in company’s Human Resources development plan, as well as in medium to long- term strategy (increase/decrease of personnel in connection with new technologies);

Medium: regular costs, i.e. wages;

I.2. Technical Resources Costs

Values: high - low

High: purchase (one-time cost), installation of new equipment;

Low: regular maintenance, ad-hoc repairs;

II. Profit

Values: Low - Medium - High

This is a relative category, based on the increase/decrease of ticket sale-related profit due to effectiveness of the Human Resources/technical measures (e.g. decrease in fare evasion);

III. Effect on Customer Satisfaction

Values: low - high; Direction: negative - neutral

This category is related to the effect the measure will have on:

- 1) customer satisfaction
- 2) level of acceptance (decrease in negative salience, passenger complaints);

In the first version of these requirements, corresponding to deliverable D3.2, WP5 suggested some methodological approaches to the proposed case studies from the tactical-operational and strategic scenarios were done by partner URJC. In this deliverable the approach is built around the economic models for the scenarios.

Based on the scenarios described in this report, some examples of various relevant aspects are enumerated, mainly grounded on the principal-agent analysis, which can be applied to WP6. The first is about the explicit incentive mechanism, the second concerns a free riding problem, and the last is an incentive problem in the relationship between TMB and outsourced companies.

The first aspect is related with the explicit incentive mechanism; the provision of explicit incentive motivates employees better, and hence improves the efficiency of an organization. Explicit incentive contracts in the form of financial and other incentives including performance-based pay have therefore been employed in both public and private sectors. These mechanisms are widely applied in the private sector, but in the public sector these performance-based schemes have not been used frequently. In the case of TMB and specifically in the security staff it is very complex and controlling an employee's behaviour becomes very costly.

The second aspect has to do with a free riding problem. In the public sector including urban public transport, performance data of employees is often accessible only at an aggregate level rather than an individual level. Team-based production and rewards can be a solution for mitigating the agency problem. However, in the situation where the production of final output depends the efforts exerted by team members, team members are likely to free ride. In the case of TMB, much of the security activities are conducted by joint actions of security guards and patrols. Since it is difficult to observe their efforts in joint actions at an aggregate level, they may give them an incentive to shirk (i.e., free ride).

Regarding the third aspect, it is related to a mal-incentive problem caused by the relationship between the transport operator and outsourced security companies. The crucial aspect of this practice is that the incentives of the operator (i.e., TMB) and the agents (i.e., outsourced companies) do not always coincide. In the economic literature, while there have been various types of agent's behaviour that must be controlled in this



type of relationship (e.g., free riding and successive monopoly), a mal-incentive problem is much more pervasive.

REFERENCES

- [1] TMB, “Basic data 2012,” TMB, Barcelona, 2012.
- [2] F. Maestre, “Psicología delictiva,” *Cienciapolicial - Technical journal from the Spanish National Police*, vol. 35 to 60, no. 35, May/July 2008.
- [3] A. M. Gómez, “Prospective Intelligence-based Security (WP) - Elcano,” 6 11 2006. [Online]. Available: http://www.realinstitutoelcano.org/wps/portal/rielcano_eng/Content?WCM_GLOBAL_CONTEXT=/elcano/elcano_in/zonas_in/defense+security/dt24-2006. [Accessed 27 11 2013].
- [4] E. R. Stroie and A. C. Rusu, “Security Risk Management - Approaches and Methodology,” *INFORMATICA ECONOMICA*, vol. 15, no. 1/2011, pp. 228-240, 2011.
- [5] SNCF, “Campaña “No hay incivismo pequeño”,” *Vía Libre*, 10 December 2012.
- [6] G. González, “Los Mossos y la Urbana intensifican su lucha contra los robos en el metro,” *El Mundo*, 08 July 2012.
- [7] J. Lee, “UTA launches new safety campaign in light of many accidents,” *Deseret News*, 16 November 2011.
- [8] C. N. Fink, B. D. Taylor and A. Loukaitou-Sideris, “From Policy and Response to System Design and Operations: Inter-Governmental Transit Security Planning in the U.S.,” *The Journal of Public Transportation*, vol. 8, no. 4, p. 1 to16, 2005.
- [9] N. G. La Vigne , SAFE TRANSPORT: SECURITY BY DESIGN ON THE WASHINGTON METRO, U.S. National Institute of Justice.
- [10] R. Goodfellow, “Lighting as a Situational Approach to Preventing Transit Crime,” in *Rail Transit Conference Proceedings*, June 2005.
- [11] CIS - Centro de investigaciones sociológicas, *Barómetro de marzo 2012 - Estudio 2935*, Madrid, 2012.
- [12] UITP, “Safety and Security of passengers in Metro Networks,” 2005.
- [13] R. Ortega, “Solo guards improve user relations at TMB,” *Public Transport International*, no. N°2 March/April 2009, 2009.
- [14] European Parliament and Council, *DIRECTIVE 2004/49/EC of 29 April 2004, Railway Safety Directive*, 2004, pp. Article 2, Scope.
- [15] Catalanian Parliament, *LLEI 4/2006, de 31 de març, ferroviària*, DOGC, 2006.
- [16] TMB, *Reglament de viatgers de Ferrocarril Metropolità de Barcelona, SA*, Barcelona, 2010.
- [17] J. Q. Wilson y G. L. Kelling, «Broken Windows: The police and neighborhood safety,» *The Atlantic Monthly*, March 1982.
- [18] E. Figueredo, «Un jutge prohibeix a un carterista entrar al metro,» *La Vanguardia*, 25 January 2013.
- [19] J. Subirats, “L’iceberg de la seguretat,” *Àmbits de Política i Societat*, no. Spring, p. 18 to 20, 2003.
- [20] D. Torrente, “La nova inseguretat ciutadana,” *Àmbits de Política i Societat*, no. Spring, p. 21 to 23, 2003.
- [21] L. Poussa, M. Räikkönen, M. Jähi, T. Rosqvist, H. Kortelainen, R. Molarius and VTT, D3.3 Urban public transport requirements final version | version 0.20 | page 71/104

“D2.5 - Report on workshop user needs and requirements,” ValueSec Project, 2011.

[22] “Delinquency and vandalism in public transport,” in *European Conference of Ministers of Transport*, Paris, 1989.

[23] UITP, “Public Transport Security in Stations,” October 2007.

8. ANNEX 1. Xarxa 4 in the context of the Barcelona metro network

As it can be appreciated in Figure 16, Xarxa4 corresponds to the central node of Barcelona Metro network.



Figure 16. Xarxa4 in the context of Barcelona metro network in the period 2011-2012

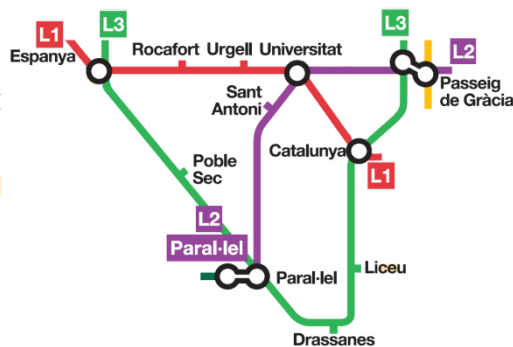


Figure 17. Detailed map of Xarxa4



It comprises four metro lines, L1, L2, L3, and L4, seventeen stations -old and new-, five line transfers to the same operator, five transfers with two other rail operators sharing neighbouring facilities and one operation tail (end of line) where trains are parked.

More detailed information about Xarxa4 can be found in report *D3.2 Urban public transport requirements first version*, section *8.2.1 Description of Xarxa4 metro network*.

9. ANNEX 2. Internal validation

According to the validation plan for Local and Regional Transport Case Study, described in D7.1-Validation Plan, the following Test Description and Workplan was defined for the first year of the project, that is, the definition of requirements phase.

Stakeholders Needs Identification					
M1-M3	M4-M5	M3-M6	M5-M6	M7-M9	M10-M12
Stakeholders Identification and Preliminary Contacts-	Urban public transport Security Needs Definition - Focus Group with transport Stakeholders	Scenarios Definition - Interviews with TMB Stakeholders , Literature and projects Review.	Scenario Validation and High level requirement definition	High-level Requirements Definition - Consortium Partners (End Users and Domain Experts) Ethnographic approach.	High-level Requirements Review - Interviews and focus groups with Public transport Stakeholders and End User Partner

The process conducted to perform the internal validation followed the established plan, but the actual activities differed in the form, but not in the content, from the initial plan.

Period	Activity	Process / Activities
M1-M3	Stakeholders identification and preliminary contacts	Identification of Stakeholders jointly with TMB
M4-M5	Urban public transport Security Needs Definition	Interviews with TMB Stakeholders
M3-M6	Scenarios Definition	<ul style="list-style-type: none"> Interviews with TMB Stakeholders (TMB internal meetings) Focus Group with transport Stakeholders (Workshop in TMB, Barcelona - June 2012)
M5-M6	Scenario Validation and High level requirement definition	First version of requirements produced by TMB. Internal review
M7-M10	High-level Requirements Definition	Presentation to Consortium Partners (General Assembly in Madrid - November 2012)
M10-M12	High-level Requirements Review	UITP Commission on Security meeting (Munich - November 2012) - Presentation of project goals and definition of high-level requirements and scenarios. Questionnaire on high-level requirements

Description of specific activities developed with external stakeholders

Focus group (workshop) held in in Barcelona on 7th June 2012

It was attended by the following personnel:

- Michael Pellot, TMB, Seconomics - Project leader
- Ricardo Ortega, TMB Security area, Seconomics project member
- Daniel Villegas, TMB Security area, Seconomics project member
- Enrique Dominguez, TMB Metro Safety Officer
- Antonio Sanchez, Regional police, Transport división (Mossos d'Escuadra)
- Martina de Gramatica, UNITIN, Seconomics partner
- Woohyun Shim, UNITIN, Seconomics partner
- Petra Gausini, SOC, Seconomics partner
- Virginia Franqueira, SecureNOK, Seconomics partner
- Silvia Castellvi, Atos, Seconomics partner
- Jaime Martin Perez, Atos, External to the project (VALUSEC project)

The following material was used during the workshop to support the scenarios definition discussion. Conclusions were feed into the first version of requirements produced.

Summary of the slides used during the workshop:

SECONOMICS WP3 Urban Transportation Case Study

Slide 2:

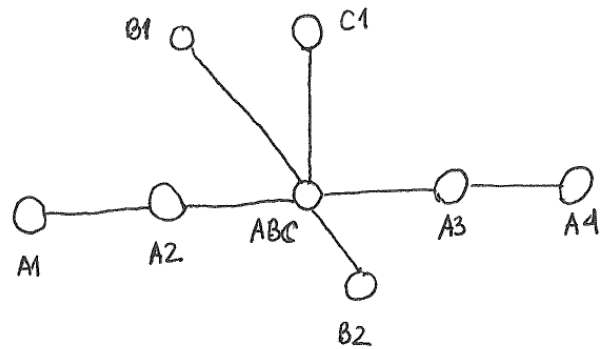
- Description

The following slides describes a case study which retains most of the essence of that an urban transport (metro) (UT) operator needs to face, as far as security is concerned. Details and data are fictitious to preserve confidentiality (and for security reasons). The study is structured in a way that an UT provider may insert their own details and undertake their own computations if required.

Slide 3:

- Description of AAA metro network. Graph

The enclosed graph describes the metro network of AAA, with the nodes (stations) and arcs (tracks).



Slide 4:

- Description. Relevant links

The enclosed table lists the relevant data concerning the relevant metro links.

Node A	Node B	Underground time	Surface time
A1	A2	10	15
.....
A3	A4	12	25

Slide 5:

- Description. Relevant stations

The enclosed table lists the relevant data concerning the relevant metro stations.

Node A	Number of entrances	Average daily passengers	Number of cameras
A1			
....			
A4			

Slide 6:

- Description. Current security resources
 - Guards (all external employees).
 - Solo guards
 - Teams and team supervisors
 - Mobile response teams
 - Security and sniffer dogs (NB. Difference?)
 - Training and coordination of actors

Slide 7:

- Description of AAA metro network

The enclosed table lists the relevant data concerning current security resources (Global, Per station, On trains,...)

Number of security (private)	Number of sniffer dogs	Number of cameras

Slide 8:

- Scenario description

The direction of AAA Metro network is worried about recent changes in security trends within the system, specially taking into account changes in the socio-economic background.

It is especially concerned with several threats described below. Most of them are ‘traditional’ but they have seen an increase in rate of occurrence, but some of them are fairly recent. Some of them affect directly the business; others potentially affect business, through image deterioration.

Slide 9:

- Scenario description

WORDS on SOCIOLOGICAL PERCEPTION OF RISK. Petra
Possibly based on the MTB survey

Slide 10:

- Scenario description

AAA Metro currently spends ***** euros in security. Given the situation, the direction of AAA Metro network has created an additional budget of ***** euros to be spent this year.

We want to:

1. identify how to best allocate such resources so as to improve the security situation:
 1. reduce likelihood and impact of threats
 2. If happening, best recover from attack
2. identify how to best display such resources (e.g. decide the random routing of guards)

Slide 11:

- Scenario decision makers and objectives

The Decision makers (DMs) in this case will be:

The DMs are specially concerned with the increase of security threats, given the more difficult socio-economic environment. They rely on the broken window theory of criminology (if nothing is done, the situation will escalate)

Slide 12:

- Scenario decision makers and objectives

The stakeholders in this case will be:

(SOME WORDS ON THEIR RISK PERCEPTION)

Slide 13:

- Scenario objectives

The identified objectives for the security resource allocation process are:

- To minimize security costs.
- To minimize costs in relation with incidents
- To minimize number of incidents of various types
- To

Slide 14:

Threats

The following types of threats have been identified. They will be described in detail below.

- Threat 1. Anti-social (Organized, coordinated and planned activities)
 - Fight, graffiti, organized vandalism,...
- Threat 2. Un-social (Unorganized threats, impulsive action)
 - (Instinctive) fare evasion,....
- Threat 3. Criminal
 - Pickpocketing, organized fare evasion,....

Slide 15:

- Threat 1. Anti-social behavior (Organized, coordinated and planned activities)
- Description:

Vandalism and graffiti deteriorate the feeling of security, reduce reliability and service quality. Repairing the assets is very expensive and transport operations are clearly affected.

For the first time, in April 2012 customers were informed about a one hour service interruption due to people invading tracks => had an immediate effect on public and pressure on policy-makers.

- Specific threats: graffiti, organized vandalism.
- Motivation: thrill-seekers, European-wide phenomena. It is not simple vandalism: it is anti-system behavior. It is a trend related with the current situation
- Stakeholders: insurance, customers
- Known groups performing the threats:???

Slide 16:

- Likelihood:
 - No. of incidents per time unit, groups attacking, locations,.....
 - Graffiti caught,...
- Impact:
 - Costs for cleaning the trains,
 - Quality service decreases: service is affected.
 - Social image: customers feel less secure.

Slide 17:

- Countermeasures for threat 1
- C1.1: Protect the trains and facilities
 - Describe how this is done
 - Cost ‘per unit’ deployed
 - Impact over Threat
 - Over likelihood of being attacked
 - Over impact of attack, if performed
 - C1.2: Inform the metro users that these acts has a cost.
 - Describe how this is done
 - Cost ‘per unit’ deployed
 - Impact over Threat
 - Over likelihood of being attacked
 - Over impact of attack
 - C1.3 Change the law (Current law too soft, but politicians do not see the problem)
 - Describe how this would be done
 - Cost ‘per unit’ deployed
 - Impact over Threat
 - Over likelihood of being attacked
 - Over impact of attack

Slide 18:

- Threat 2. Un-social behavior
- Description:

Unorganized and impulsive actions. Penalties if found - 50€ on the spot and 100€

 - Specific threats: fare evasion, accidents (i.e. escalators)
 - Motivation: Save money
 - Stakeholders: insurance, customers,

Perpetrators. Nonpaying customers and fare evasion club

Slide 19:

- Likelihood
 - 3.2% fraud estimate
 - 4,6 Million inspection (2011, 60.000 penalties)
 - Profile of offenders? Do they pay immediately?....
 - Impact:
 - Financial loss. (ticket inspections increases the income of the company).
 - Social image (Fare evasion decrease radically the feeling of security, ticket inspection increase customer satisfaction).

Slide 20:

- Countermeasures for threat 2
- C2.1: Federation team asking for ticket in a platform.
 - Describe how this is done
 - Cost ‘per unit’ deployed (costs for control and legal costs). But earnings through fines

- Impact over Threat
 - Over likelihood of being attacked
 - Over impact of attack, if performed
- C2.2: Technological measures: Automatic access doors.
 - Describe how this is done
 - Cost ‘per unit’ deployed
 - Impact over Threat
 - Over likelihood of being attacked
 - Over impact of attack, if performed

Slide 21:

- Countermeasures for threat 2
- C2.3: Portable inspection devices (tickets readers)
 - Describe how this is done
 - Cost ‘per unit’ deployed
 - Impact over Threat
 - Over likelihood of being attacked
 - Over impact of attack, if performed
- C2.4: Organizational measures (communication plan & customers information: poster, flyers).
 - Describe how this is done
 - Cost ‘per unit’ deployed
 - Impact over Threat
 - Over likelihood of being attacked
 - Over impact of attack, if performed

Slide 22:

- Threat 3. Criminal
- Description:

Pickpocketing and anti-social behavior

- Threats: sleepers, tramps, antisocial behavior against customers

(Huge typology of incidents, NB can we specify a bit more)

- Motivation: criminal
- Stakeholders:
- Perpetrators:

Slide 23:

- Likelihood
 - No. of events of various types per month, per station, globally,...
 - Times of day, carriages, passengers on carriage,...
- Impact
 - Social image: pickpocketing and anti-social behavior decreases the feeling of security radically.
 - Security costs. NB: Meaning???
 - Impact of mass media in the public security.

Slide 24:

- Countermeasures for threat 3.

- C3.1 Technological measures: Video surveillance and security control center.
 - Describe how this is done (Does it already exist? You mean a better one?)
 - Cost ‘per unit’ deployed
 - Impact over Threat
 - Over likelihood of being attacked
 - Over impact of attack, if performed
- C3.2 Technological measures: Radio equipment & Geo-localization
 - Describe how this is done (Already implemented? More units?)
 - Cost ‘per unit’ deployed
 - Impact over Threat
 - Over likelihood of being attacked
 - Over impact of attack, if performed

Slide 25:

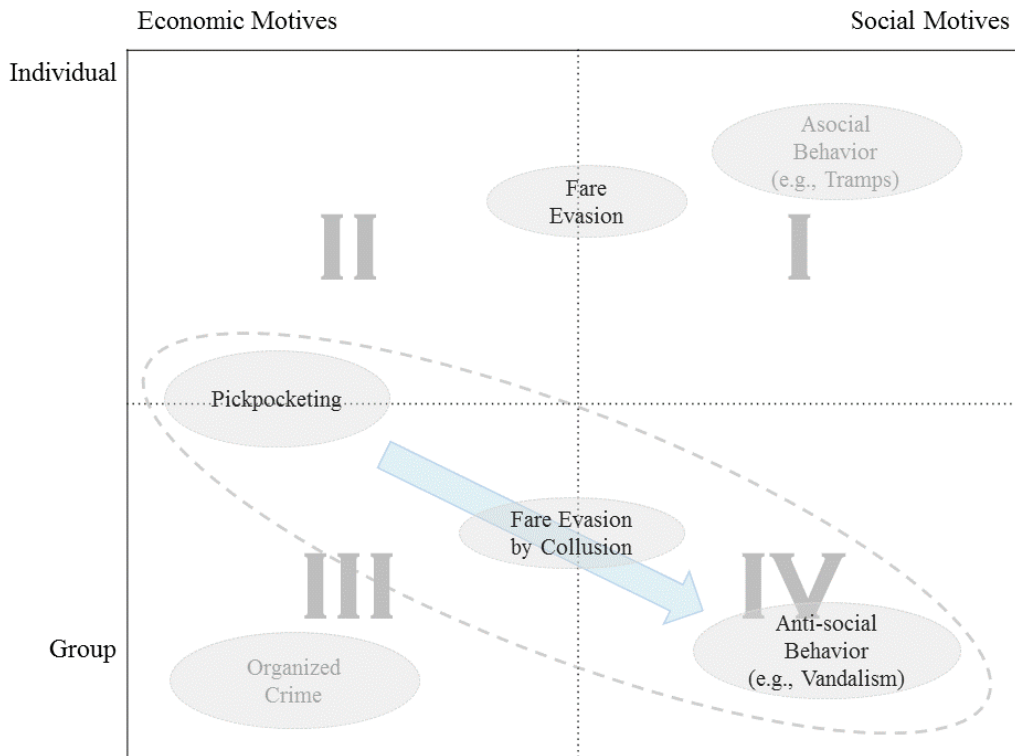
- Countermeasures for threat 3.
 - C3.3 Organizational measures: Random routes of patrols
 - C3.4 Organizational measures: Random routes of solo-guards and dogs
 - C3.5 Organizational measures: Coordinated actions with dogs
 - Describe how this is done (Already implemented? More units?)
 - Cost ‘per unit’ deployed
 - Impact over Threat
 - Over likelihood of being attacked
 - Over impact of attack, if performed
 - C3.6 Organizational measures: Criminal prosecution (AAA) Process
 - Description: They detect the criminals and communicate to the police office, and try to take the criminals out of the metro (the dog help to it).
 - Cost ‘per unit’ deployed
 - Impact over Threat
 - Over likelihood of being attacked
 - Over impact of attack, if performed

Slide 26:

- Countermeasures for threat 3.
 - C3.7 Organisational measures: Customer information: sensibility plan (posters, flyers).
 - Describe how this is done
 - Cost ‘per unit’ deployed
 - Impact over Threat
 - Over likelihood of being attacked
 - Over impact of attack, if performed

Slide 27:

The following graph provides a global view of the problem



Slide 28:

We aim at dealing with the three threats simultaneously in that:



- The three are considered important by AAA.
- There is a single budget to deal with all of them.
- Countermeasures may have effects on various types of threats simultaneously, as shown in the next table

Slide 30:

- Problems to be tackled
1. identify how to best allocate such resources so as to improve the security situation:
 1. reduce likelihood and impact of threats
 2. If happening, best recover from attack
 2. identify how to best display such resources (e.g. decide the random routing of guards-dogs)
 3. Appropriate fining scheme
 4.

High-level requirements review during the UITP Commission on Security meeting held in Munich on 7th and 8th November 2012

It was attended by the following personnel:

 			
UITP Security Commission			
14th Meeting – Munich			
6-8 November 2012			
List of participants			
CHAIRMAN			
Thomas	KRITZER	WIENER LINIEN GMBH & CO KG	Austria
HONORARY CHAIRMAN			
Geoff	DUNMORE	LONDON UNDERGROUND LTD	United Kingdom
VICE CHAIRMAN			
Ricardo	ORTEGA	FERROCARRIL METROPOLITA DE BARCELONA	Spain
LOCAL HOST			
Rainer	COHRS	MUNCHNER VERKEHRSGESELLSCHAFT	Germany
MEMBERS			
Antonin	FEDORKO	DOPRAVNI PODNIK HLM PRAHA AS	Czech Republic
Jiri	SUBRT	DOPRAVNI PODNIK HLM PRAHA AS	Czech Republic
Patrick	DILLENSEGER	REGIE AUTONOME DES TRANSPORTS PARISIENS	France
Yoshiharu	TAKEUCHI	EAST JAPAN RAILWAY COMPANY (FRANCE)	France
Kiyohiro	TAKEMOTO	EAST JAPAN RAILWAY COMPANY	Japan
Carolin	BÜTTNER	DEUTSCHE BAHN AG	Germany
Mirco	MEWES	HAMBURGER HOCHBAHN-WACHE GMBH	Germany
Hans Martin	RUDOLPH	HAMBURGER HOCHBAHN-WACHE	Germany
Ingo	TEDERAHN	BERLINER VERKEHRSBETRIEBE	Germany
Ali	ABDOLLAHPOUR	TEHRAN URBAN & SUBURBAN RAILWAY CO	Iran
Pierluigi	PELARGONIO	ATAC S.P.A.	Italy
Cristiano	STIFINI	ATAC S.P.A.	Italy
Bernetta	HARTING	HTM PERSONEN VERVOER NV	Netherlands
Michael	PELLOT	TRANSPORTS METROPOLITANS DE BARCELONA	Spain
Sergey	BOBROV	MOSCOW METRO	Russian Federation
Vladimir	RODIONOV	MOSCOW METRO	Russian Federation
Dmitry	ZAEMSKY	MOSGORTANS	Russian Federation
Douglas	ZEIGLER	MTA NEW YORK CITY TRANSIT	United States of America
GUESTS			
Yves	PERREAL	THALES TRANSPORTATION SYSTEMS	France
OBSERVERS			
Jacques	COLLIARD	UNION INTERNATIONALE DES CHEMINS DE FER	France
Greg	HULL	AMERICAN PUBLIC TRANSPORTATION ASSOCIATION	United States of America
Reinhard	RUNNE	COLPOFER	France
Ulrich	WEBER	VDV	Germany
UITP			
Denis	LUYTEN	UITP	Belgium
Lindsey	MANCINI	UITP	Belgium
Natacha	WHITE	UITP	Belgium

05/12/2012

During this meeting, dissemination activities were carried out, with the presentation of a project summary, project consortium and work package structure. The Urban Transportation Case Study was also presented with information on the different scenarios defined. The current status of the work was detailed, and further contributions to Expert Group for joining the next Stakeholders Workshop were requested.

A questionnaire was distributed among assistants, mainly metro operators, to gather feedback on high-level requirements. Conclusions collected from this questionnaire have been consolidated in the main deliverable.

Attached, the questionnaire used during the meeting, and a summary of survey answers. Conclusions were feed into the first version of requirements produced.

The following presentations were used during the workshop to support the scenarios definition discussion.

Summary of the slides used during the meeting:

PROJECT PRESENTATION SOCIO-ECONOMICS MEETS SECURITY

Slide 2:

SECONOMICS goal is **synthesizing sociological, economic and security science** into a usable, concrete, actionable knowledge for policy makers and social planners responsible for citizen's security.

Slide 3:

The project is **driven by industry case studies** and will specifically identify security threats in transport (air and urban and super urban metro) and critical infrastructure. The research focus places social science and political science at the heart of the modeling framework.

Slide 4:

In particular the project **seeks to explore the challenges of pan European coordination in security outcomes** for transport and critical infrastructure.

Slide 5:

The contribution of the project will be in **developing and furthering the state of the art in modelling security problems** in a technological and socio economic context and then applying state of the art risk assessments and analysis of the social context to develop optimal policies.

Slide 6:

The **outputs** are twofold:

First **assessment of the future and emerging threats in the identified areas** with rigorous modeling of the optimal mechanisms for mitigation within the policy domain.

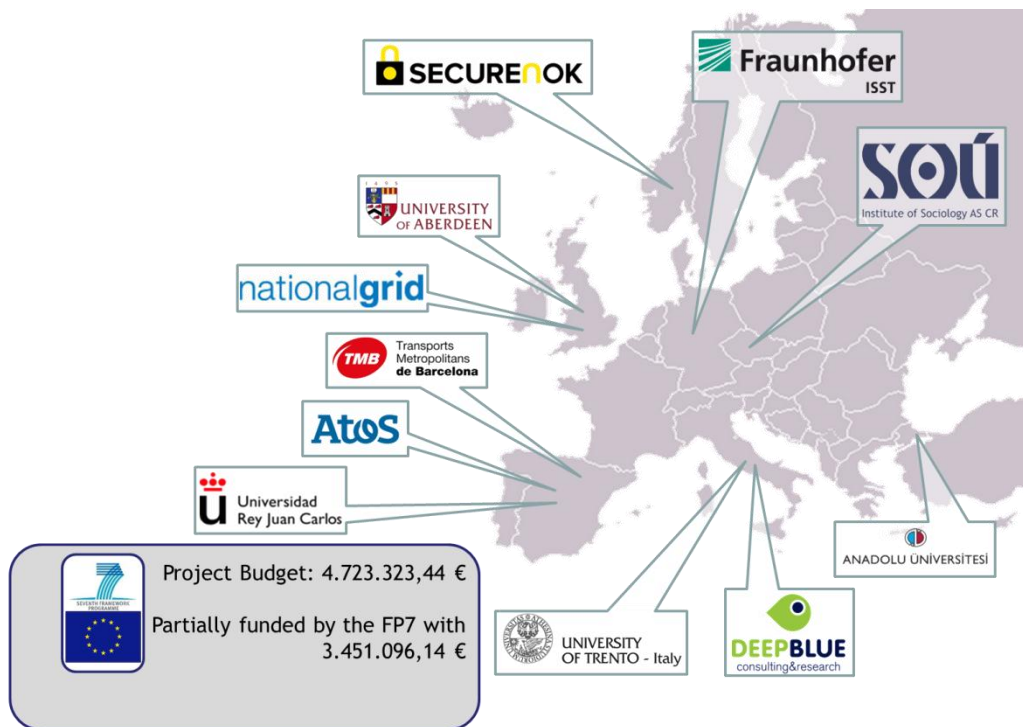
Second, and more crucially, a **generalized policy "toolkit" that will assist decision makers in identifying and reacting coherently** (within the appropriate social context)

to future and emerging threats that may arrive long after the project has been completed.

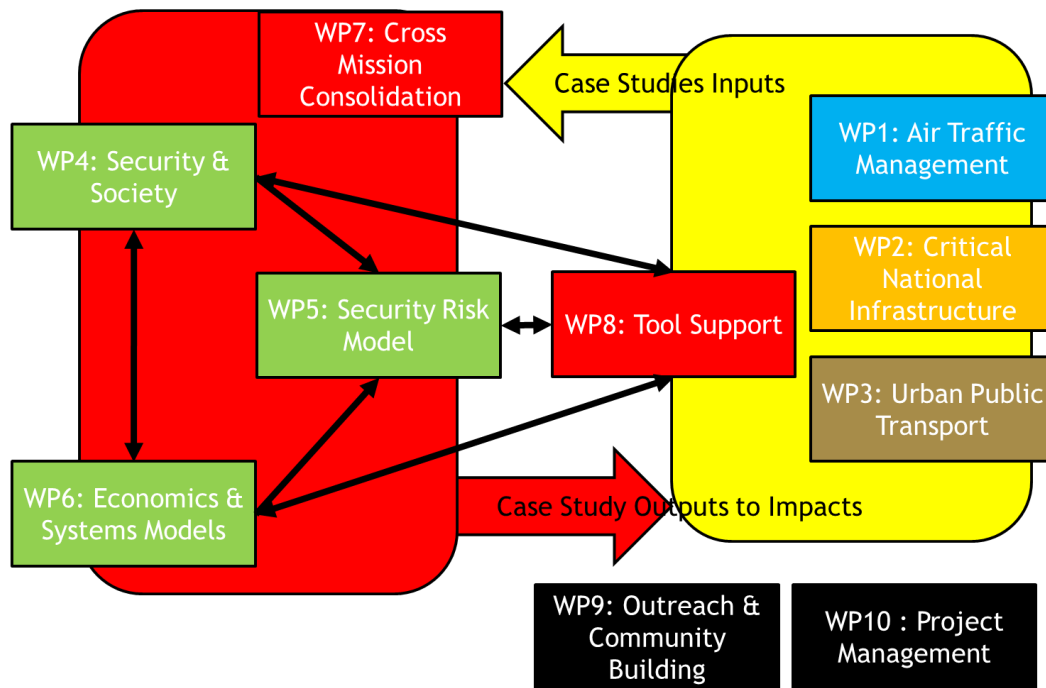
Slide 7:

The lasting impact of SECONOMICS will be a **methodological revolution** driven by a **common, but diverse set, of modelling tools and utilizing recent advances in modelling technology that seamlessly transverses the social, economic and technological domains.**

Slide 8:



Slide 9:



**SECONOMICS WP3
Urban Transportation Case Study**

Slide 2:

TRANSPORT USE CASE OBJECTIVES

- Research how policy makers can improve awareness about society perception of public transport security.
- Investigate the optimal mechanisms for implementing security policy.
- Investigate the economical impact of policies.
- Investigate the impact of social preferences.

Slide 3:

TRANSPORT USE CASE OBJECTIVES

- To support design of socio-economic model that will be developed in WP4, WP5 and WP6 (Socio-economic research) assuring the representation of public transport.
- They have awareness that exist a clear relation between public information about security in the medias (newspapers, tv, internet and others) and the end users perception of public transport security.
- WP3 will support WP4 on assessing the society view and evaluation of the urban public transport security.

Slide 4:

TRANSPORT USE CASE SCENARIO DESCRIPTION

- The following slides describes a case study which retains most of the essence of that an urban transport (metro) provider needs to face as far as security is concerned.

- Details and data are fictitious to preserve confidentiality and for security reasons.

Slide 5:

TMB THREATS

Barcelona workshop in TMB

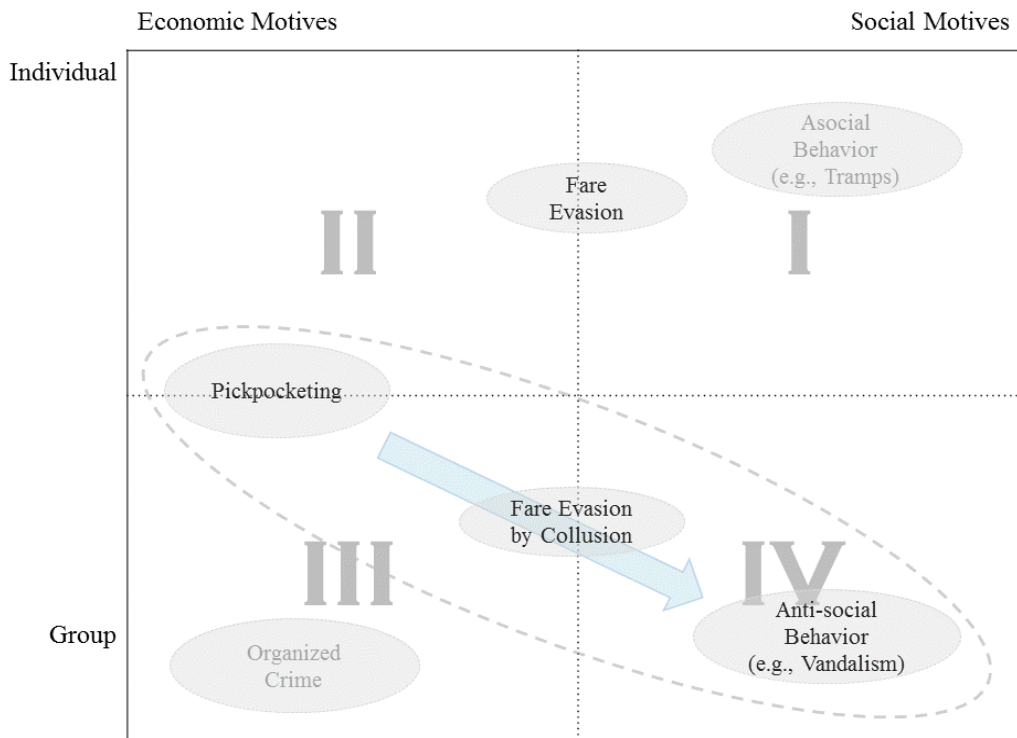
It was celebrated a workshop with partners, TMB security members and regional police.

During the Barcelona workshop the following threats had been identified.

- Scenario 1: Anti-social
- Scenario 2. Un-social
- Scenario 3. Criminal

Slide 6:

SCENARIOS ANALYSIS



Slide 7:

SCENARIOS ANALYSIS: Unsocial behavior

Unsocial behaviour (Type I) can be defined as the lack of consideration for public property and public rules resulting in damages to established safety and security.

Unsocial behaviour (Type I) shows the lack of consideration for others, which can result in emotional or physical harm.

Slide 8:

SCENARIOS ANALYSIS: antisocial behavior

Antisocial behaviour (Type IV) can manifest in various forms and intensities such as breaking formal rules and laws.

Antisocial behavior (Type IV) which can be represented by organized vandalism is very important and interesting because it becomes more aggressive and has huge impact on the public's perception of security

Slide 9:

SCENARIO 1. VANDALISM AND GRAFFITI: Anti-social behaviour (Type I)

Threats:

- Graffiti's, organized vandalism.

Motivation:

- Thrill-seeking; enjoyment and peer recognition (no monetary profits).

Impact:

- Costs is around 100.000€/year;
- Indirect costs: estimated on 1% loss in traffic (feeling of insecurity);
- Quality service decreases: service is affected;
- Social image: customers feel less secure.

Slide 10:

SCENARIO 2. FARE EVASION by Individuals or by Collusion

Threats:

- New trend: fare evasion by collusion (i.e., between passengers or between passengers and employees).

Motivation:

- Traditional forms: economic motives (e.g., saving money);
- Joint fare evaders: social reasons (e.g., social bonding).

Impact:

- Fare evasion has resulted in enormous financial losses to TMB;
 - Social image: decrease the feeling of security radically;
 - Ticket inspection: increases customer satisfaction.

Slide 11:

SCENARIO 3. PICKPOCKETING: Individual Crime (Type III) and Organized Crime (Type IV)

Threats:

- Pickpocketing (one of the most pervasive), drug transaction, harassment and robbery.

Motivation:

- criminal and economic;

Impact:

- Security costs;
 - Social image: decrease the feeling of security radically;
 - Impact of mass media in public security.

Slide 12:

SCENARIO 4. TRAMPS: Un-Social Behaviour (Type II)

Threats:

- Tramps (or sleepers);
- During 2011: 1.090 tramp cases;

Motivation:

- Unsocial emotions;

Impact:

- Security costs;
 - Social image: tramps and sleepers decreased the feeling of security radically.

Slide 13:

COUNTERMEASURES APPLIED IN DIFFERENT THREATS

Countermeasures	Threats			
	Vandalism and Graffiti	Fare evasion	Pickpocketing	Tramps
Protect trains and facilities	X			
Inform the users, communication plan	X	X	X	
Change the law	X			
Ticket inspection		X		
Ticket readers		X		
Automatic access doors		X		
Pentalties	X	X		
Video surveillance	X		X	X
Security control center		X	X	X
Radio equipment & geo.localization			X	X
Patrols			X	X
Solo guards and dogs			X	X
Coord. Actions with dogs			X	X
Collaboration with police authorities			X	X

Slide 14:

SOCIAL PERCEPTION OF SECURITY AND RISK

- Social perception of security and risk analysed in WP4.
- Risk perception is studied as a targeted attitude to specific types of risks:
 - Unsocial behavior
 - Antisocial behavior

Slide 15:

SECURITY REGULATORY FRAMEWORK

- An increasing pressure to standardize and regulate.
- It is difficult to balance: applications-risk-budget.
- local authorities are responsible of security regulation.
- How to proceed? To share best practices and recommendations.

Slide 16:

RISK ASSESSMENT METHODOLOGIES

- **Strategic scenarios**

The strategic scenarios require the use of game theoretic concepts. We might view this as a sequential defend-attack problem.

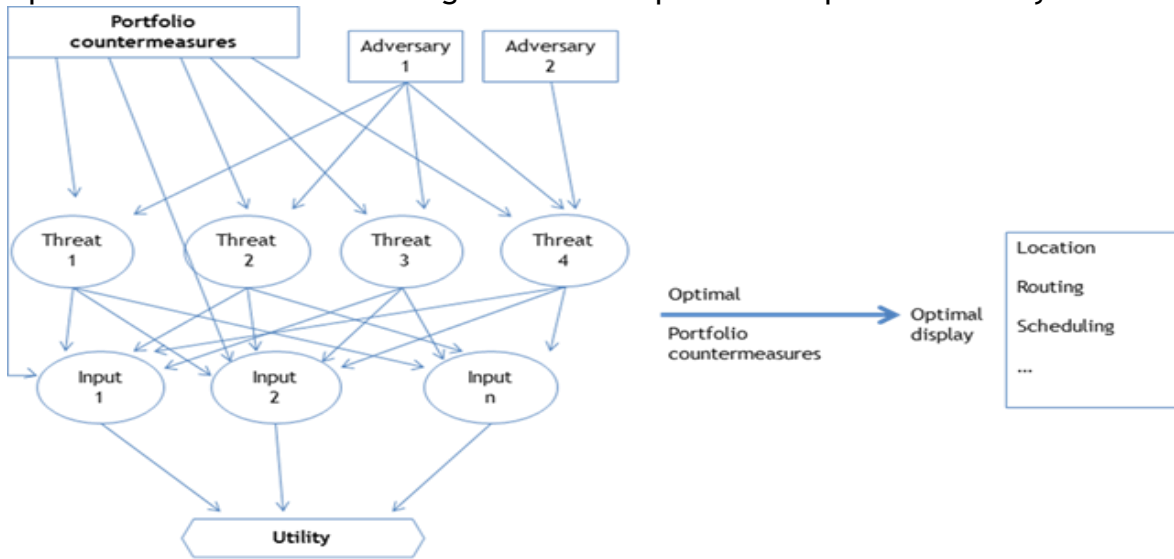
- **Tactical-operational scenarios**

The proposed tactical-operational scenario may be described as a security resource allocation problem. It may be solved, in principle, within the risk analytic framework.

Slide 17:

TACTICAL-OPERATIONAL SCENARIOS

Operational Scenarios Modeling in the Urban public transport Case Study



Slide 18:

YEAR 1: WHERE WE ARE

- Done:
 - WP3:
 - D3.1: Ethical opinion/authorization (M3)
 - First Workshop with local stakeholders (lack of users representatives) (M6)
 - D3.2: Urban public transport Requirements - first version (M6)
 - Overall:
 - Cross mission consolidation (today in Madrid within Consortium meeting)
- Under development:
 - WP3:
 - Survey within Metro operators (today!)
 - Constitution of an Expert Group (Volunteers are welcomed!)
 - Second Workshop with the Expert Group (Beginning 2013)
 - D3.3: Urban public transport requirements - final version (Beginning 2013)



Questionnaire Security concerns in Urban Transport

SECONOMICS “Socio-Economics meets Security” (Contract No. 285223) is a Collaborative project) within the 7th Framework Programme, theme SEC-2011.6.4-1 SEC-2011.7.5-2 ICT.

This questionnaire presents some questions related to the requirements gathering for the Public Transport scenario for the development of the SECONOMICS framework and tools.
You are invited to contribute to this assessment in the course of the SECONOMICS urban public transport security framework analysis.

I - Security decision-making

Q1. What describes best, the approach your organization has towards security?

(single choice)

- Strategic: Organization focused, addressing the causes - proactive
- Operational: Asset/incident focused, addressing the symptoms - reactive
- Others. Please, detail:
-
-

Q2. What are the priorities when addressing security-related decisions in your organization?

(multiple choice - rate priority of selections: 1- top priority; 2, 3, ... - less priority)

- Passenger’s security perception
- Passenger’s real security
- Facilities security
- Information security
- Cost
- Others. Please, detail:
-
-



Security Economics: Socio economics meets security



Q3. Who are the stakeholders that have influence in the security decision-making?

(multiple choice - rate the influence of stakeholders: 1- most influence; 2, 3, ... - less influence)

- Citizens
- Local, regional or state politicians (parliament members, mayors)
- Public authorities (ministries, local authorities, agencies, emergency services, police)
- Non-governmental organizations (neighbourhood associations, civic associations)
- Firms and consulting companies (advisers, specialists, consultants)
- Organization personnel
- Others. Please, detail:
-
-

Q4. Which are the main societal impacts taken into account in the security decision-making in your organization?

(multiple choice - rate priority of selections: 1- top priority; 2, 3, ... - less priority)

- Ethical: interference in private matters, company's ethical guidelines
- Environmental: e.g. usage of environmental friendly materials (e.g. extinguishing media) or limiting the amount of non-environmental friendly ones
- Societal: social structure, unemployment rate, citizens satisfaction, neighbourhood complaints
- Economic: losses due to decrease of activity, costs versus benefits
- Political: public image of the party/politician, political state of affairs, recent political events
- Legal: previous court decisions, EU standards and principles
- Safety: public safety e.g. safety of the participants of mass events'
- Internal acceptability / company policies: Handling the subject in personnel working group (impact on working surroundings) and necessary expert groups (impact on respective area). Impact on daily work
- Acceptability: public acceptance, customer approval (client's opinion)
- Others. Please, detail:
-
-



Q5. Which are the biggest challenges in the security decision-making process?

(multiple choice - rate priority of selections: 1- top priority; 2, 3, ... - less priority)

- Availability of data /information about the security threat
- Timeframe for the decision making process and the implementation of security measures
- Process, influence of different stakeholders and different perspectives of the security problem
- Others. Please, detail:
-
-

Q6. What are the most important dependencies that influence the security decision-making?

(multiple choice - rate priority of selections: 1- top priority; 2, 3, ... - less priority)

- EU and national legislation, international agreements
- Organizations' internal procedures
- Previous decisions (made by other stakeholders and own organization)
- Experience
- Current political and economic atmosphere (restrictions)
- Social atmosphere
- Press and media
- Available information
- Guidance and advices (other authorities, consultants)
- Time constraints
- Political actors involved (politicians, parties and administrative actors)
- Company surroundings and functions
- Risk assessment/risk analysis
- Resources (trained and capable personnel, budget).
- Others. Please, detail:
-
-



II - Data requirements and evaluation of security measures

Q7. What are the ways used to calculate the cost and benefits of the decision security measures?

(multiple choice - rate priority of selections: 1- top priority; 2, 3, ... - less priority)

- Intuition: Intuition together with factual information and experience
- Qualitative analyses: Costs and benefits are assessed in political and social terms. Estimations what might happen without certain preventive measures
- Quantitative tools: Financial assessment, use of e.g. occupational health statistics
- Others. Please, detail:

III - Strategic requirements

Q8. Which aspects should require some Standard/European regulations for improving the security in public transport?

(multiple choice - rate priority of selections: 1- top priority; 2, 3, ... - less priority)

- Standard procedures and measures to manage common risks
- Minimum security measures according to passenger volume
- Passenger regulation
- Design of transport infrastructures
- Others. Please, detail:



IV - Tool requirements

Q9. What would be the main requirements for the support tool developed?

(multiple choice - rate priority of selections: 1- top priority; 2, 3, ... - less priority)

- Usability: Easy to use, understandable (e.g. risk calculation), avoid complicated training, easy and low maintenance (avoid troubles and extra costs), self-explanatory, no high expert design
- Interoperability: Possibility to integrate the data/results with other existing systems (programs and data bases), permanent access to most of the updated data is an important aspect
- Flexibility / Tailoring: Possibility to (easily) tailor and further develop the tool according to the organization's own specific needs. To be able to implement new capabilities easily. Different user profile options (policymaker, manager, head of security, expert on specific matter/area)
- Data security: High information security. Control of information feed and access
- Documentation/reporting: Graphic visualisation of the findings. Comparing measures and their costs
- Low equipment needs: Low operating cost. Availability for different operating systems. Web-based tool rather than software based service (platform independent)
- Reliability: Reliability of used databases / information
- Others. Please, detail:

Q10. What are the most important factors that the support tool should be able to report?

(multiple choice - rate priority of selections: 1- top priority; 2, 3, ... - less priority)

- Societal impacts
- Risk: Total risk. Different values of sub-risks. Risk reduction
- Measures: Prioritise measures. Show and suggest how security measures reduce risks. Present measures which are needed to lower the risks in possible scenarios. Show the available measures
- Costs
- Effects: Negative effects which could be avoided, Different effects depending on the selected measure
- Scenarios: Alternative scenarios ("what will happen when...")
- Weighting: Balance between risk and effect reduction and the costs to achieve that reduction
- Display of output: Graphs, scenarios, tables, ranges and short explanations. Tables and ranges (e.g. colour coded „traffic lights“) would enable an easy comparison of values/results/options
- Others. Please, detail:

Following is a summary of the answers received to the previous questionnaire, according to the priority assigned to each answer. The total number of choices for each answer is also reported. As all questions except Q1 where multiple choices, the total amount of answers for each question depends on the selection each survey respondent has made, being the maximum six possible answers, as that was the total number of respondents.

I - Security decision-making questions

Q1. What describes best, the approach your organization has towards security?		
Answer ranking	No. of answers	Answer
1	4	Strategic: Organization focused, addressing the causes - proactive
2	2	Operational: Asset/incident focused, addressing the symptoms - reactive
n/a	-	Others

Q2. What are the priorities when addressing security-related decisions in your organization?		
Answer ranking	No. of answers	Answer
1	5	Passenger's real security
2	6	Facilities security
3	5	Passenger's security perception
4	6	Information security
5	6	Cost
6	1	Others: For facilities we focus on critical infrastructure and proactive security measures

Q3. Who are the stakeholders that have influence in the security decision-making?		
Answer ranking	No. of answers	Answer
1	6	Local, regional or state politicians (parliament members, mayors)
2	5	Organization personnel
3	4	Citizens
4	3	Public authorities (ministries, local authorities, agencies, emergency services, police)
5	2	Non-governmental organizations (neighbourhood associations, civic associations)
6	1	Others: Statistics and survey, Questionnaires
n/a	-	Firms and consulting companies (advisers, specialists, consultants)

Q4. Which are the main societal impacts taken into account in the security decision-making in your organization?		
Answer ranking	No. of answers	Answer
1	6	Internal acceptability / company policies: Handling the subject in personnel working group (impact on working surroundings) and necessary expert groups (impact on respective area). Impact on daily work
2	5	Legal: previous court decisions, EU standards and principles
3	4	Safety: public safety e.g. safety of the participants of mass events'

4	4	Societal: social structure, unemployment rate, citizens satisfaction, neighbourhood complaints
5	4	Economic: losses due to decrease of activity, costs versus benefits
6	4	Acceptability: public acceptance, customer approval (client's opinion)
7	4	Ethical: interference in private matters, company's ethical guidelines
8	2	Political: public image of the party/politician, political state of affairs, recent political events
9	1	Environmental: e.g. usage of environmental friendly materials (e.g. extinguishing media) or limiting the amount of non-environmental friendly ones
n/a	-	Others

Q5. Which are the biggest challenges in the security decision-making process?

Answer ranking	No. of answers	Answer
1	6	Availability of data /information about the security threat
2	5	Process, influence of different stakeholders and different perspectives of the security problem
3	4	Timeframe for the decision making process and the implementation of security measures
4	1	Others: Establishing a clear business case and benefit of security decisions

Q6. What are the most important dependencies that influence the security decision-making?

Answer ranking	No. of answers	Answer
1	5	Organizations' internal procedures
2	4	Current political and economic atmosphere (restrictions)
3	4	Available information
4	4	EU and national legislation, international agreements
5	4	Previous decisions (made by other stakeholders and own organization)
6	4	Political actors involved (politicians, parties and administrative actors)
7	3	Risk assessment/risk analysis
8	2	Experience
9	3	Press and media
10	2	Company surroundings and functions
11	2	Resources (trained and capable personnel, budget)
12	1	Time constraints
13	1	Social atmosphere
n/a	-	Guidance and advices (other authorities, consultants)
n/a	-	Others

II - Data requirements and evaluation of security measures questions

Q7. What are the ways used to calculate the cost and benefits of the decision security measures?

Answer ranking	No. of answers	Answer
1	6	Qualitative analyses: Costs and benefits are assessed in political and social terms. Estimations what might happen without certain preventive

		measures
2	6	Quantitative tools: Financial assessment, use of e.g. occupational health statistics
3	5	Intuition: Intuition together with factual information and experience
n/a		Others

III - Strategic requirements

Q8. Which aspects should require some Standard/European regulations for improving the security in public transport?		
Answer ranking	No. of answers	Answer
1	5	Minimum security measures according to passenger volume
2	3	Passenger regulation
2	2	Standard procedures and measures to manage common risks
3	1	Others: Minimum standards for Security Risk Assessment
3	1	Design of transport infrastructures

IV - Tool requirements questions

Q9. What would be the main requirements for the support tool developed?		
Answer ranking	No. of answers	Answer
1	6	Usability: Easy to use, understandable (e.g. risk calculation), avoid complicated training, easy and low maintenance (avoid troubles and extra costs), self-explanatory, no high expert design
2	5	Flexibility / Tailoring: Possibility to (easily) tailor and further develop the tool according to the organization's own specific needs. To be able to implement new capabilities easily. Different user profile options (policymaker, manager, head of security, expert on specific matter/area)
3	5	Interoperability: Possibility to integrate the data/results with other existing systems (programs and data bases), permanent access to most of the updated data is an important aspect
4	4	Documentation/reporting: Graphic visualisation of the findings. Comparing measures and their costs
5	3	Reliability: Reliability of used databases / information
6	2	Data security: High information security. Control of information feed and access
7	2	Low equipment needs: Low operating cost. Availability for different operating systems. Web-based tool rather than software based service (platform independent)
n/a	-	Others

Q10. What are the most important factors that the support tool should be able to report?		
Answer ranking	No. of answers	Answer
1	6	Measures: Prioritise measures. Show and suggest how security measures reduce risks. Present measures which are needed to lower the risks in possible scenarios. Show the available measures

2	4	Effects: Negative effects which could be avoided, Different effects depending on the selected measure
3	5	Display of output: Graphs, scenarios, tables, ranges and short explanations. Tables and ranges (e.g. colour coded „traffic lights“) would enable an easy comparison of values/results/options
4	3	Weighting: Balance between risk and effect reduction and the costs to achieve that reduction
5	3	Risk: Total risk. Different values of sub-risks. Risk reduction
6	3	Costs
7	2	Societal impacts
8	2	Scenarios: Alternative scenarios ("what will happen when...")
n/a	-	Others

10. ANNEX 3. Glossary

This a specific glossary for terminology used in the context of urban transport and urban transport security.

A

Antisocial behaviour.

Behaviour of an organized nature and / or intentional or recidivist involving violations of criminal or administrative regulations with a clear social disdain.

C

Criminal behaviour.

Behaviour defined in the criminal laws in force.

L

Law enforcement officer.

Person to who is attributed a number of legal rights and duties in relation to the functions carried out within his professional field; it can be both public and private domains.

O

Objective security.

Situation corresponding to the number of crimes and / or antisocial incidents detected and / or verifiable within optimum ranges and social acceptance.

P

PA system.

Public Address system. Sound system used to issue voice messages in public places.

Private security.

Economic activity developed by non-institutional actors, which collaborate with the actors responsible for public security and to protect individuals and / or property.

Public security.

Set of players, mechanisms and actions on which resides the definition, regulation and maintenance of public safety.

R

Risk.

Probability of occurring damages of different levels of social and / or economic impact, on individuals and / or on tangible or intangible goods.

S

Security measure.

Human action, organizational or technical intended to prevent, mitigate, deflect or meet present or future risks against individuals or property whose aim is to achieve objective security and / or socially accepted sense of security.

Segurómetro.

TMB basic management tool which that describes spatial average of security incidents on a monthly basis, differentiating the issues affecting the sense of security and those that affect the objective security.

Sense of insecurity.

State of unrest, due to the existence of environmental factors and / or uncivic incidents, exceeding socially acceptable tolerances.

Sense of Security.

State of peace corresponding to a null or low impact of unfavourable environmental factors, uncivic incidents, and not merely the absence of criminal and / or antisocial incidents.

Social warning.

Situation that arises when the existence of criminal and / or antisocial incidents exceeds the established societal tolerance, either justified or not.

T

Threat.

Causal phenomenon of potentially dangerous situations for the safety of individuals and / or tangible or intangible goods.

TMB.

Transports Metropolitans de Barcelona. Barcelona main public transport operator. Exploits Metro network and the vast majority of bus lines in the metropolitan area of Barcelona.

U

Uncivic behaviour.



Individual and / or sporadic behaviour not adjusted to socially accepted code of conduct, which causes a state of uneasiness and discomfort in people who witness it.

V

Vulnerability.

Degree of potential exposure to risk in relation to the resilience of people and / or facilities affected.

11. ANNEX 4. Detailed information on security incidents and resources

In a separate Addendum “Detailed information on security incidents and resources in the Barcelona metro network”, specific information about incidents and security resources is provided considering the whole network and the specific part of the network chosen for this study, Xarxa4, which is the portion of the Barcelona Metro network being considered for the scenarios described in this report.

The document that contains this information is classified as CO; Confidential, only for members of the consortium (including the Commission Services); as it contains sensible information that it is not convenient to be disseminated broadly.