SECUR-ED

SECured URban transportation - European Demonstration

D55.1 Preliminary best practices

Document identification	
Related SP / WP	SP5 / WP55
Related Deliverable	-
Lead Participant	CRTM
Contributors	UITP SPs Leaders

Reference	SCR-WP55-D-CTM-005
Dissemination Level	PU
Lead Author	Tomás Melero Nuria Blanco Antonio García
Reviewers	FOI RATP MTRS PMB and experts

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

History

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

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

Version	Status	Date	Author	Main Changes
0.1	Draft	15.07.2013	CTM	First internal draft
0.2	Draft	12.09.2013	CTM	Second internal draft
0.3	Draft	20.10.2013	CTM	Third internal draft
0.4	Draft	01.01.2014	CTM	Fourth internal draft
0.5	Draft	15.01.2014	CTM	Fifth internal draft
1.0	Under review	24.01.2014	CTM	Version sent to peer reviewers (Uploaded on the **Cooperation Tool**)
1.1.	Under review	04.02.2014	THA	Version sent to PMB and experts for peer review
1.2.	Under review	14.02.2014	CTM	Changes due peer reviewers
1.3.	Under review	21.02.2014	CTM	Changes due peer reviewers
2.0	Under review	19.03.2014	CTM	Reviewed version (Uploaded on the **Cooperation Tool**) for final check
3.0	Under review	24.03.2014	CTM	Updated version with SP3 contribution
3.1	Under review	27.03.2014	THA	Revised version following PMB comments
3.2	Under review	31.03.2014	CTM	Updated version with other documents list. Sent for final quality check
4.0	Issued	31.03.2014	THA	Submitted version uploaded on SESAM

TABLE OF CONTENTS D55.1

1 Abstract & Purpose

1.1 Summary

This document has been created in order to identify preliminary best practices for security management inside urban transport environments and determined within the European project SECUR-ED.

For the elaboration of this document the basis has been all of the documents produced during the project to date. A key contributing factor has been the full support and clarifications of the partners who contributed to their content. In addition, other reference documents identifying best practices in public transport, produced in other projects, have been analysed.

The information contained in this document will provide the basis for future documents and manuals based on the best practices produced within SECUR-ED.

1.2 Purpose of the document

During the development of SECUR-ED a number of capacities (solutions that comprise both technologies and operational best practices) have been studied and developed with the objective of improving public transport security.

These studies have produced many different results. Some of them will be tested in the real environments of flagship and satellite demonstrations in order to assess their benefits and applicability.

The purpose of this document is to review the project in order to highlight the best practices anticipated within SECUR-ED.

1.3 Scope and limitations of the document

This document is preliminary to the consolidation of the flagship demonstrations results.

As a consequence, this is a study based on all the documents created to date and the opinion of experts in order to collect the most promising solutions.

- The evaluation of the various solutions and studies presented inside the project do not take into account their experimentation via the demonstrations and the associated results.
- There are no quantitative results to study. The selection of the highlighted results has been based on qualitative sources and opinion of experts.
- The conclusion of this document must be contrasted with the ones obtained after the flagship demos and the rest of the documents related to project results.

2 References

2.1 List of acronyms

BPMN	Business Process Modelling Notation
CBRN-E	Chemical Biological Radiological Nuclear Explosives
CCTV	Closed Circuit Television
DoW	Description of Work
HMI	Human Machine Interface
IT	Information Technology
N/A	Not Applicable
OCC	Operational Control Centre
PT	Public Transport
PTO	Public Transport Operator
RFID	Radio Frequency Identification
SCADA	Supervisory Control and Data Acquisition
SECUR-ED	Secured Urban Transportation – European Demonstration
SOA	Service Oriented Architecture
SP	Subproject
SW	Software
UITP	International Association of Public Transport
WP	Work Package

2.2 Referenced documents

The following documents are referenced:

R[1] SCR-WP21-D-JRC-006-11 D21.1 - A glossary of public transport security terminology & definitions

R[2] SCR-WP21-D-MTR-011-09 D21.2 - Survey on current public transport operators security practices

R[3] SCR-WP21-D-MTR-004-11 D21.3 - Overall approach to security management and emergency preparedness

R[4] SCR-WP22-D-FHG-002-05 D22.1 - Interoperability concept

R[5] SCR-WP31-D-MTR-018-08 D31.1 - State of the art preparedness approaches for pt operations

R[6] SCR-WP31-D-HCO-025-07 D31.2 - Best practices for conducting risk assessments

R[7] SCR-WP31-D-HCO-024-05 D31.3- Inventory of awareness raising and competence

building activities

R[8] SCR-WP31-D-EDI-055-02 D31.4 - Risk assessment tool SRS.

R[9] SCR-WP32-D-MPH-013-03 D32.1 - Comprehensive solution for protection of passengers facilities

R[10] SCR-WP32-D-NIC-007-02 D32.2 - Integrated model type solution for train protection solution

R[11] SCR-WP32-D-ATM-018-05 D32.3 - Generic solutions for protection of line of route infrastructure

R[12] SCR-WP35-D-THA-010-04 D35.1 - Operator data exchange capacity

R[13] SCR-WP35-D-THA-021-07 D35.2 - I2PIS : Individualized passenger information capacity

R[14] SCR-WP35-D-FHG-015-04 D35.3 -Proof-of-concept demonstrator for post-event analysis

R[15] SCR-WP35-D-INO-016-02 D35.4 - Cyber defense capacity

R[16] SCR-WP35-D-BOM-008-18 D35.5 - Telecommunications

R[17] SCR-WP36-D-BOM-030-01 D36.5 - Intelligent early warning tool for decision support

R[18] SCR-WP37-D-MTR-013-04 D37.1-Emergency & Crisis preparedness handbook (Part 3 - Specific scenarios response plans)

R[19] SCR-WP38-D-WUE-006-08 D38.1 - Training organisation and management

R[20] SCR-WP38-D-MTR-038-04 D38.3-Training programmes for security employees (ST001)

R[21] SCR-WP38-D-MTR-108-05 D38.4 - Training programmes for operators in control centres (OT001)

R[22] SCR-WP38-T-DBA-069-03 D38.5- Training programmes for security managers

R[23] SCR-WP38-D-MTR-112-01 D38.6 - Emergency and crisis exercise planning guidance

R[24] SCR-WP41-D-ANS-002-11-D41.1 - Preliminary Architecture and Set of ICDs

R[25] SCR-WP41-D-THA-011-03-D41.2 - Detailed architecture and set of ICDs

R[26] SCR-WP41-D-THA-013-04 D41.3 - Interfaces compliance and validation report

R[27] SCR-WP51-D-HCO-001-04 D51.1 - Guideline to conduct a security audit

R[28] SCR-WP51-D-ANS-003-03 D51.2 - Experimentations building manual

R[29] SCR-WP52-D-ALS-013-02 D52.7- Summary of analysis

R[30] SCR-WP54-D-JRC-001-05-D54.2 - Assessment of Capacities Considered in SECUR-ED

R[31] SCR-DOW-C-THA-001-03 - Grant Agreement Annex I DoW

R[32] SCR-WP11-D-UIP-008-01 - D11.1 State of the Art on Security and Privacy Policies

R[33] SCR-WP11-D-UIP-033-01 - D11.2 Measures to improve security and privacy

R[34] Selección de ejemplos de buenas prácticas en accesibilidad universal en el transporte público. Consorcio Regional de Transportes de Madrid. Área de movilidad y accesibilidad.

R[35] Transport interchange best practices Buchann,C.DETR

R[36] A guide to best practices for achieving context sensitive solutions.National research council (Estados Unidos); transport research board

R[37] Intermodal Transport Interchange for London: best practices guidelines. Transport for London

R[38] Hacia un sistema integrado de información de transportes; restos- soluciones- buenas prácticas. Consorcio Regional de Transportes de Madrid; Unión Internacional de Transportes Públicos

R[39] Manual de buenas prácticas para proyectos: planificación y financiación, claves en la gestión de tranvías. La voz de Atuc

R[40] La planificación conjunta de los usos del suelo y transporte al servicio del desarrollo urbanos sostenible; una guía de buenas prácticas. Monzón de Cáceres, Andrés; López Lambas, María Eugenia

3 Preliminary best practices characteristics

3.1 Parameters to be considered

A best practice is a method or technique that has consistently shown results superior to those achieved with other means, and that is used as a benchmark. Best practices are used to maintain quality as an alternative to mandatory legislated standards and can be based on self-assessment or benchmarking.

For the study of preliminary best practices contained within SECUR-ED some characteristics have been defined bearing in mind the objectives for this deliverable described in the SECUR-ED Grant Agreement DoW for WP55-Best Practices Materials:

"The aim of this WP is to summarize previous tasks […], in order to establish the answers to "how, when, where, what and by who" best practices at PT system level.

Best practices will have four common characteristics:

- *To be innovative.*
- *To make a difference as to improve the security level.*
- *To have a sustainable effect as being industrial and maintainable over the transit system life cycle.*
- *To have the potential to be generic enough in order to serve as a model for generating initiatives elsewhere (instantiation)."*

Those that fulfil the characteristics mentioned above will be considered as preliminary best practices.

The points below describe the selected best practices parameters and the most important characteristics of them to enable selection as preliminary best practices.

3.1.1 Be innovative

Be innovative refers to the following aspects:

- Based on new technologies.
- Based on previous technologies (introducing some innovation on it).
- Applied to environments where it has never applied so far.

3.1.2 Improvement of the security level

Improvement of the security level involves the following aspects:

- Be quantifiable.
- Improve the risk assessment hence risk management capability.
- Improve the security level in: prevention, response to the receipt of threats, post incident response, post incident analysis,feedback ...

3.1.3 Reusable

Be reusable refers to the adaptability of the capacity to different environments than that for which it was designed, with slight or no modification. More precisely, be reusable refers to:

- Facility of using new technologies, methodologies and functionalities in different situations.
- Common language for all the stakeholders involved (public transport operators, public transport authorities, users, emergency services, first responders...)
- Modularity
- Interoperability.
- Standardisation.

3.1.4 Application in real environments

Application in real environments involves a series of aspects related to the use of the capacity under typical mass transport conditions.

- Minimum cost.
- Same functionalities as those proven in the demonstrations and with the same characteristics.
- Scalability (from medium size cities to large metropolitan areas).
- Reliability.
- Availability.
- Maintainability.
- Safety.

3.1.5 Characteristics diagram

These characteristics have been analyzed in both a qualitative and quantitative way. Qualitative information is provided by a description of the practice´s features directly related to the parameters.

On the other hand, a quantitative analysis is also provided for each best practice as an output by means of a bar diagram which includes the parameters analyzed and their classification as Low-Medium-High.

	Low	Medium	High
Be innovative			
Improvement of the security level			
Reusable			
Application in real environments			

3.2 Methodology

The methodology used for the development of this deliverable is based on the analysis of all previous factors in order to determine which capacities identified during the SECUR-ED project may be defined as best practices prior to the demonstrations. Information required to apply this methodology is found in the following:

- Studies of the documents developed within SECUR-ED.
- Questionnaires.
- Studies of the points of view about best practices given by the SPs leaders.
- Analysis of other reference documents about best practices in public transport.

The results obtained in this document give a preliminary overview about the most relevant results obtained during the development of SECUR-ED.

3.2.1 SECUR-ED deliverables and documents

63 of the 108 deliverables of SECUR-ED were identified as important for the development of the project conclusions.

33 deliverables issued at that time contributed to the study.

They are referenced inside §2.2 from R[1] to R[33].

The remaining deliverables to be issued will be part of the final conclusions.

3.2.2 Questionnaires

A second step to fully understand all the practices/methodologies/activities carried out during the SECUR-ED project in order to recognise the key issues was to consult the experts in each sub-project and analyse the documents that have been realized in their field of action.

In the frame of different analysis inside SECUR-ED project, some questionnaires were distributed to work-package leaders and other experts. The analysis of the answers to these questionnaires allowed to assess the various solutions according to the following extended parameters list :

- Risks addressed by the capacity: This describes the risks/threat that the practice is mainly intended to handle. In addition, it indicates whether the capacity is very specific to mass transportation and to these risks, or if it has broader uses.
- Suitability for mass transport security: This factor focuses in the difficult conditions in urban mass transport, such as very large number of people, activities in many locations, mobile platforms, etc. The parameter shows how the capacity fits with the security purpose.
- Legal, societal and ethical acceptability: this parameter analyses the possible legal or regulatory constraints regarding the use of the practice. It also focuses on concerns about the acceptability of the capacity in the users and ethical concerns, mainly privacy and fundamental human rights.
- Effectiveness: This parameter describes how the capacity reduces the main risks identified in the first point. The description is normally based on comparisons to existing risk levels, or comparisons to other solutions handling the same risk. In

addition, the effectiveness is also related to other positive effects -lowering staff costs, increasing passengers' comfort, reducing delays, etc.- and negative effects -passenger discomfort, false alarms requiring staff interventions, etc.

- Maturity: Maturity studies the level of development of the capacity. This parameter analyses if the capacity has been available for a long time or if it is an innovation. Maturity also reviews, if there is any organization supporting the capacity or if it has a proven track record in both the general market and the specific mass transportation environment.
- Flexibility: The flexibility parameter analyses the scalability of the capacity. It focuses on the changes in equipment, infrastructure or personnel that the capacity would require to be applied in other types of city. It also takes into account the regional, organisational and cultural differences that may affect the security procedures.
- Costs: This parameter evaluates the acquisition costs for the capacity, including costs for development, procurement, test and validation, integration and training, as well as expected operation and maintenance costs. Costs also includes whether benefits or cost savings could be achieved by applying the capacity.

These factors provide a first global view of the solutions studied within the project and help to obtain a global knowledge about the different practices. The answers to the questionnaires were interpreted according to the 4 parameters defined in §3.1: innovation, security improvement, reusable and application in real environments. The information may be classified as follows:

➜ Innovation

- o Elements that have been generated in the project itself (totally innovative). This point includes the application fields as well as the development.
- o Elements based on a previous practice. This point includes the application fields and the improvements that the element provides.
- o Where the innovative element is located (process, object, context...).

➜ Improvement of the security level

- o Contents that lead to a notable improvement of the security level when they are applied.
- o Potential users of the element: public transport passengers, public transport staff, emergency services, organisation responsible for application, security equipment industry for application development.
- o Aspects in which the elements improve the security level: early alarm, decrease in response time, minimising of the affected area, less risk to users, staff or infrastructure, improving the decisions management...
- o Within this point, it is also important to include if the elements have been tested and which aspects have been used in those tests.

➜ To be reusable

- o Possibility to use the practice/methodology/activity in different environment than that in which they have been applied.

  - Possibility to modify the practice/methodology/activity in order to adapt it to different environments.
  - Possibility to transfer the results obtained to any transport means, including different size, different transport, different users...
  - Some of the contents of different SPs have already been applied on different environments. In such case, this point will include the different environments in which the practice has been applied, the obtained results or the adaptation required for each environment.

- Application in real environments
  - Most relevant results from the practices that have already been carried out.
  - Conditions of use that differ to those initially defined.
  - Final users of the practice/methodology/activity.
  - Degree of acceptance of the practice/methodology/activity and different analyses or studies carried out in order to understand the acceptance by final users.

Relation between WP54 and WP55 characteristics

	Be innovative	Improve the security level	Reusable	Application in real environments
Risk addressed by the capacity		X		
Suitability for mass transport security				X
Legal, societal and ethical acceptability				X
Effectiveness		X		
Maturity	X			
Flexibility			X	
Costs				X

3.2.3 SPs leaders point of view about best practices

Some extra best practices were collected from the points of view of SPs leaders.

These best practices are not necessarily deliverables or capacities, but extra nuggets that have helped the project advance, or will be helpful to the sector after the project, over and above the defined official project deliverables.

The identified points are those appearing in the table below:

Basic	**Risk assessment guidelines (D31.2, D31.4)** Although not demonstrations as such, the risk assessment guidelines developed in SECUR-ED were implemented successfully in 9 public transport networks. It is widely agreed that a security risk assessment is the first step in developing a coherent security policy and both the guidelines and software tool have been developed to be used autonomously by public transport operators.
	Security audit checklist (D51.1) To complement a risk assessment, the security audit is a useful tool to discover the current state of affairs of security in a network from a more qualitative point of you. This simple checklist, used in the risk assessment process in the 9 networks mentioned above, is a helpful addition for public transport operators.
	Overall approach for security (D21.3) Although not “demonstrated” as a capacity as such, this document was widely used by the satellite demonstration cities as a helpful reference when designing the demonstrations as it gives a good, concise overview of public transport security practices.
	Public Transport Security Terminology & Definitions (D21.1) This glossary of terms comprises general safety and security terms, relevant IT terms as well as public transport terms, making it a very useful reference document.
	Ethical checklist To prepare the demonstrations, each demonstration city was obliged to comply with a variety of ethical and privacy rules on the local, national and European level. In order to accompany the teams through this process, the ethical checklist was developed, to make sure all legal and ethical issues were properly addressed. Although developed specifically for the project, the checklist would be useful for any public transport operator when implementing new security policies, measures or technologies.
	Rely as much as possible on international standards for minimum interoperability requirements Provided it limits itself to the minimum requirements necessary to perform a mission, standardization has a series of advantages as improving performance, reducing risks, encouraging innovation, becoming more sustainable and saving costs. Practically, a security standard is a document established by international consensus and promulgated by an independent body, in response to a recognized need of harmonization or interoperability to improve security. It is usually a formal document that establishes uniform criteria, procedures or methods.
	Be able to share a common time and geo-location (including within underground infrastructures)

	Machines, like humans, need for understanding each other to be able to answer in a same way to the three basic questions “what, where & when”. This common understanding means sharing a data model for all the events necessary to address a security situation. Events themselves can be extremely varied, but being able to reliably consider their sequence means that they are all time-stamped with a same common clock, practically the universal time (UTC). To relate to physical world they need to be associated to a unique location; this is achieved today easily in open air through the GPS coordinates, but remains a challenge in 3D structures, especially underground where GPS signals cannot be received and no mapping standard exists
	Contribution to standardization As a direct conclusion of the above two items, it is of common interest to SECUR-ED stakeholders to transform the best practices developed in the project into doctrines defining the minimum requirements to succeed in a mission. In most cases, such doctrines will prove to be shared by the pairs faced with the same situations worldwide and standardization by consensus in the relevant international bodies can start.
	Interoperability framework (SOA) specifications Through Event Driven and Service Oriented Architecture SECUR-ED has reached loose coupling in the demonstrated security solutions. The solutions can be easily reused and orchestrated independently from each other. Another positive effect is the testability and consequential improvement for maintenance and modular expandability.
Nuggets to prepare the project	**Workflows with BPMN** Working with 42 Partners from different countries, industries, and with diverse technical-, business-, educational-, and cultural- backgrounds; clear communication has been of utmost importance. Early in the project, it was discovered that BPMN (Business Process Modelling Notation) helped eliminate much miscommunication; moreover, it helped bridge an understanding between those that were more business/management minded and those more focused on the technical details. BPMN 2.0 was ultimately decided as the standard notation to be used by all demonstrations for defining their respective demonstration scenarios. (Coincidentally, BPMN 2.0 was also introduced into ISO/IEC 19510 in 2013) In the context of SECUR-ED, the model’s primary elements included: “Swimming lanes” which represented responsibilities and locations like Security Operation & Control Centre, Crisis Management, onboard, platform, public authorities; with naming conventions consistently used. “Start Node” which represented a unique identified system event. Starting from a single start node, the process would be branched out with conditional and parallel “Gateways” to represent situational workflows. “Activities” represented different types of actions; which primarily helped represent messages between systems, manual instructions, human interaction, executionof a program.

	Ultimately, each process can have multiple “End Nodes” corresponding to different situational outcomes. BPMN revealed to be a perfect tool for collaboration between members with business and technical background. Particularly it also helped map out the interactions and processes behind human and software interfaces; providing an easy visual of the message flow between “service” providers and consumers. BPMN Modeling is just a first step to a complex Event Processing and Decision Making Framework. For the more advanced users associated with software development, the execution of BPMN could be extended to the use of Rules Engines for the complex Event Processing; which was less explored in the context of SECUR-ED.
	Integration through SOA The interchange and distribution of relevant information in real time, particularly in managing security events in rapidly changing situations, is supported by having a common software architecture design pattern. Particularly pertinent to software integration, in conjunction with the PROTECTRAIL project, Service Oriented Architecture (SOA) was decidedly used in SECUR-ED with a focus on eventing to support integration efforts; particularly at the sensor level to the visualization. This architectural approach essentially enables the “services” exposed by one system that uses a SOA to be interacted by another system. Thus making a number of capacities easily reusable in various configurations required by each demonstration, and in the larger set of applications in the industry. The event based SOA approach proved to be a good base for commonality and modularity, and provided the associated flexibility that can be controlled to avoid any unwanted change of configuration that is crucial in security applications.
	Cost and benefit analysis on capacities and on solutions The current economic crisis in the EU area– coupled with a perceived reduced level of attention on terrorism risks - is forcing stakeholders to reduce their investments in security. It is therefore crucial to run cost and benefit analysis (CBA) on both the single capacities and the integrated solution. From all demonstrations it becomes evident that proposed solutions (and in particular physical installations) cannot limit themselves to protect against terrorism but shall address to improve the CBA ratio, as much as possible, also the so called High Probability Low Impact (HPLI) events – like vandalism, copper theft, etc. – and possibly cover also safety issues (e.g. yellow line trespassing, crowd management, etc.).
	Analysis of country specific privacy and legal barriers Many demonstrations have encountered difficulties in the management of privacy and legal barriers for what concerns the implementation of capacities. This has been particularly emphasised for CCTV analytics and CBRNE devices. The different demo cities have experienced • Ambiguities in the national legislation

	• Differences between legislations of the capacity provider and the legislation of the country of the demo (with the need of changes in the capacity itself to adapt it to the destination country) • Differences between privacy legislation at the EU level and those at the national level.
Improving Security Culture	**Physical and cyber security cannot be separated any more (from risk assessment by organizations and implementations)** As processing technologies can be found at every level in public transportation systems and as this pervasive penetration grows as legacy systems are replaced by modern solutions, the cyber vulnerabilities apply to all assets. The traditional segregation between information systems and the isolated operational “safe-by-design” systems has vanished. This means that when a security problem occurs to a system, cyber and physical malicious origins have a probability of occurrence. This has an obvious impact on the technical implementations, but also on the organizations.
	Side benefits of conducting a risk assessment & security audit The direct benefits of conducting a risk assessment and security audit are described above, however there are many indirect benefits from using such an approach, for example: ○ Improving security awareness throughout hierarchy ○ Persuading decision-makers of need to invest ○ Establishing or improving relations with external stakeholders
	Combined safety and security use of solutions The current economic crisis in the EU area is forcing stakeholders to reduce their investments in security and identify smarter solutions for bypassing this problem. Most of the capacities tested and validated in SECUR-ED have the possibility to be used to cover both safety and security aspects thus optimising investments. This has been shown particularly in the area of people tracking and of intrusion detection.
Managing the project	**Extensive use of Advisory Groups** The project made extensive use of a number of Advisory Groups: - AG for public transport operators and authorities - AG for law enforcement and first responders - AG for industry - AG for ethical and societal issues An Advisory Board was also set up, made up of officials from a number of relevant Directorate Generals from with the European Commission as well as some non-European public transport security experts. Each AG had a slightly different role but in general the aim was to make sure the needs of all relevant stakeholders were taken into account as the project developed, to improve acceptance of project proposals and output to the widest possible range of stakeholders outside the consortium, therefore

	contributing to the European added value. The AG for law enforcement and first responders was particularly innovative as it is the first time a public transport security project has taken into account this important stakeholder. The Ethical AG was instrumental in developing the Ethical Checklist (see above).
	High profile videos To enhance dissemination, significant budget was reserved for the production of several videos. One general one, produced at the mid-way stage, aimed at outlining what the project intended to cover. More detailed videos, developed towards the end of the project, have the aim to give a concrete overview of what was developed and demonstrated during the project.
	Synergy achieved by combining key events The Mid-term and final conferences of the project are key elements for project dissemination. The project decided to organise both events in conjunction with other important sector events in order to maximise participation: - Mid-term Conference: organised in conjunction with UITP World Congress & Exhibition – this led to a high level of participation including non-Europeans - Final Conference: organised in conjunction with DG MOVE’s LANDSEC meeting of national representatives and public transport stakeholders.
	Retro-planning to prepare demonstrations events As each demonstration involved an open event for observers, a detailed event planning process was designed to be followed by each demonstration team. This process could be useful beyond the scope of the project.

3.2.4 Other documents and references

Apart from detailed study of the project, other documentary sources about best practices in public transport (other projects, articles, documents...) have been studied.

They are referenced under §2.2 from R[34] to R[40].

As a result of the analysis it is possible to have a global vision about the best practices of other projects about public transport that could give an idea about which kind of best practices SECUR-ED would produce.

4 Preliminary best practices within SECUR-ED

As commented in the previous section, the selection of best practices required a wide analysis of previous deliverables and SECUR-ED documents as well as of questionnaires collecting the point of view of experts. In addition, SP leaders also provided a general vision of some innovative practices and methodologies that have been implemented during SECUR-ED. Finally, other projects and papers regarding public transportation were consulted in order to gain more information about certain points.

The focus of the study has been the following:

- Solutions developed during SECUR-ED that will be tested in the flagship demos.
- Relevant practices and methodologies identified during the project which have helped the project advance, or which will be helpful to the sector after the project end and above the official deliverables.
- Lessons learned

Around 60 capacities have been developed inside the project (see Annex I) and most of them will be tested in four flagship demonstrations and six satellite demonstrations.

Here are the solutions for the 4 flagship demonstrations:

Madrid demonstration

SECUR-ED Deliverable	Capacity ID no.	Capacity
D35.1	INFO-01-03	Supervision Server
D35.1	INFO-02-03	Orchestration engine
D35.2	INFO-04	Passenger Information
D35.2	INFO-05	Operator work station
D33.3	CCTV-01-01	Fixed basic CCTV
D33.3	CCTV-01-03	Road vehicles onboard Basic CCTV
D33.3	CCTV-04	Person tracking in video
D31.1, D31.3	ADD-05	Organisational, operational and IT procedures & plans
D31.1, D31.3	ADD-06	Incident response plan

Paris demonstration

SECUR-ED Deliverable	Capacity ID no.	Capacities
D35.1	INFO-01-01	Supervision Server

D35.1	INFO-01-04	Supervision Server
D35.3	INFO-03-02	Post-event analysis (CCTV forensics)
D36.5	INFO-06	Decision Support System - Early Warning System
D37.3	INFO-07	Decision Support System - Restoration of Operations
D35.5	TELECOM-02	Communication between field security staff and SOCC
D33.3	CCTV-01-01	Fixed basic CCTV
D33.3	CCTV-01-02	Rail-standard basic CCTV
D33.3	CCTV-01-03	Road vehicles onboard Basic CCTV
D33.3	CCTV-04	Person tracking in video
D33.3	CCTV-07	Face recognition
		Unattended object detection
D34.2	CBRNE-01-02	Chemical Detection - AP4C
D34.2	CBRNE-01-03	Chemical & Explosives Detection - Street Lab Mobile (TICs/TIMs, explosives, narcotics, and CWAs)
D34.2	CBRNE-01-05	Radiological Detection – GAMPIX (gamma imaging system)
D34.2	CBRNE-01-06	Radiological Detection – DIRAD (automatic gamma detection system)
D34.2	CBRNE-01-07	Radiological Detection - Smart Gamma Probe (Area Monitoring and Alarm Triggering)
D34.2	CBRNE-01-08	Radiological Detection - CZT Handled Spectrometer (Miniature spectrometer)
D34.2	CBRNE-01-10	Explosives Detection - T-REX (Portable vapordetection system)
D34.2	CBRNE-01-12	Explosives Detection – SYPODEX (Vapor detection using Quartz Crystal Microbalance technology)
D34.2	CBRNE-01-13	Explosives Detection - QCL Portal PBIEDs (Personal Borne Improvised Explosive Device) Detection System
D34.2	CBRNE-01-14	Explosives Detection - Mobile TracePortable Narcotics and Explosives Detector
D35.4	CYBER-01-01	Good practice & preventive measures - Cyber

		security risk assessment model
D35.4	CYBER-01-02	Good practice & preventive measures - Information Systems Backup & Restore (procedure)
D35.4	CYBER-03-01	Incident response (mitigation/restoration) - IT Vulnerability Remediation Management (procedure)
D31.1, D31.3	ADD-05	Organisational, operational and IT procedures & plans
D23.3		Agent dispersionsimulation

Milan demonstration

SECUR-ED Deliverable	Capacity ID	Capacity
D35.1	INFO-01-02	Supervision Server
D35.5	TELECOM-01-01	Communication between vehicles and ground/wayside - via 3G/LTE/WIFI
D35.6	TELECOM-03	RFID ticket tracking
D33.3	CCTV-01-01	Fixed basic CCTV
D33.3	CCTV-01-04	Fixed basic CCTV
D33.3	CCTV-01-05	Fixed basic CCTV
D33.3	CCTV-02-01	Wayside - Detection of persons in outdoor areas supposed to be empty
D33.3	CCTV-02-02	On-board Empty Vehicle Detection (OEVD)
D33.3	CCTV-04	Person tracking in video
D33.3	CCTV-06-02	Crowd Density Detection - Wayside / Fixed Facilities
D33.3	CCTV-05	Crowd abnormal behaviour detection
D34.2	CBRNE-01-06	DIRAD Radiological materials detection
D34.2	CBRNE-01-01	Chemical & Explosives Detection - RAID-S2 (Bruker) IMS Sensor System
D32.3	CCTV-02-03	Wayside - Perimeter anti-intrusion and graffiti prevention for Depot Protection and infrastructure protection
D32.3	ADD-02	Paint Sniffer
D23.3	SIMU-01	Evacuation modelling

Berlin demonstration

SECUR-ED Deliverable	Capacity ID	Capacity
D33.3	CCTV-01-04	Fixed basic CCTV
D33.3	CCTV-01-05	Fixed basic CCTV
D33.3	CCTV-02-01	Wayside - Detection of persons in indoor areas supposed to be empty
D38.1, D38.2	TRAINING-01	Security training course for front-line employees
D38.1, D38.3	TRAINING-04	Security training course for security agents
D38.1, D38.4	TRAINING-06	Security training course for OCC operators in security command and control centres
D38.1, D38.4	TRAINING-07	Simulator training for operators of CCTV system in the security control room
D38.1, D38.5	TRAINING-08	Security training course for security managers
D38.1, D38.6	TRAINING-09	Emergency and Crisis Preparedness Training Programme: Focused exercise
D38.1, D38.6	TRAINING-10	Emergency and Crisis Preparedness Training Programme: Full-scale exercise
D31.1, D31.3	ADD-05	Organisational, operational and IT procedures & plans

The study in this deliverable has been focused on the groups or capacities which, working together, will give solutions very useful for PTOs in the resolution of security problems.

Apart from the capacities used in the scenarios some other points have been identified as proposed best practices. Some of them are complementary to the solutions mentioned before. For example, in Paris demo where the cyber security is one of the solutions implemented, experts have detected that in order to improve the security culture physical and cyber security cannot be separated any more (from risk assessment by organizations and implementations). In Madrid demo BPMN has been used in order to develop some of its solutions.

In order to cover all the project and keeping in mind that the solution of each demo involved many capacities and practices that all together will be very useful for the future, it was decided to select the most relevant practice of each demonstration.

Following this line of action the following practices were considered as best practices within the framework of the SECUR-ED project:

- Orchestration engine, as the most relevant practice of the Madrid demonstration.
- Cyber security, as the most relevant practice of the Paris demonstration.
- CBRNe sensors, as the most relevant practice of the Paris demonstration.
- Tracking, as the most relevant practice of the Milan demonstration. It was also very important during Paris demo.

- ➔ Training, as the most relevant practice of the Berlin demonstration.
- ➔ Contribution to standardization, as general SECUR-ED practice.

4.1 Orchestration engine

Short description

As defined in previous documents, an orchestration engine is a SW management tool enabling:

- Correlation of events and alarms into qualified incidents.
- Exchange of relevant information between relevant security stakeholders in the incident management process.
- Management of the incident resolution process.

Technically, this module provides:

- An ontology/semantics editor to describe the environment (ontology) and the semantics (standardised dialogues between stakeholders).
- A process editor to create or import dematerialised procedures using business processes modelling standards such as BPMN.
- A runtime to dynamically execute dematerialised procedures upon completion of trigger conditions within the SOA environment, as a service consumer.
- A Web service enabling stakeholders to interact in the incident management process, via their operator workstations, depending on their role and the corresponding granted rights.

The dematerialised procedures may be:

- Procedures to correlate events into qualified incidents/alarms.
- Procedures to exchange relevant information between relevant security stakeholders in the incident management process.
- Standard operating procedures to manage security events.

Relation with other capacities

This best practice is closely related with the *early warning systems*.

The capacity aims to detect and report events that are seen as indicators of a potential threat, thus giving time to operators to take preventive actions in order to avoid security incidents at all or their escalation.

The system operates as decision-support tool. Depending on the events of the system and corresponding configuration of decision rules (based on fuzzy logic), the system provides outputs to the human operator, informing him/her about the occurrence of these events and their operational security meaning (alert function). This will be done through dash-boards which can be configured by the user.

Advantages and answers to indirect needs for operators

- ➔ Reduce false alarms
- ➔ Increase confidence in the systems

- Reduce response time
- Improve coordination between stakeholders

Conclusions

As stated in previous points, the parameters analysed in each capacity have been the following:

- **Be innovative**

  The orchestration engine is already in an experimental stage in all areas, including that of mass transport. In this aspect, SECUR-ED will represent a proof of concept.

- **Improvement of the security level**

  The orchestration engine is a generic tool to ease implementation of security procedures, and may therefore be applied to almost any threat management. Due to the very broad possible use of the capacity (possibly automation of any security procedure) it is difficult to define how effective this capacity is in reducing risks. SECUR-ED has mainly tested the capacity as an information sharing tool (defining which information is relevant to whom and with which vocabulary). As such, the capacity is expected to be much more effective than any other procedural communication model in the case of an exceptional security incident. However, it is not certain that the capacity will be more effective than human communication through radio in organizations that are already well acquainted to multi-stakeholders cooperation.

  Short-term, the orchestration engine increases the efficiency of OCC operators, and, in particular, increases communication between stakeholders thanks to a decision support making tool. On the other hand, in the long-term it envisages increased efficiency of OCC operators and communication between stakeholders beyond the use cases managed by the system. In particular it is expected that the "multi-operator exchange capacity" will improve the cooperation between operators, law enforcers and first responders at all levels, not limited to the use of a common tool to share information.

- **Be reusable**

  The orchestration engine may be applied in different modes of mass transportation. The capacity has been designed to be adaptable to any particular arrangement between operators, first responders and law enforcement. However, such a system requires an important design investment to define and model procedures, and is therefore rather tailored for big cities with important coordination challenges.

  The integration into different stakeholders is eased by the use of a web-based HMI for operators. It may therefore be introduced easily in different control rooms of a city without major investment. However, the orchestration engine assumes that other security capacities being orchestrated are available with modern SOA interfaces, which is not necessarily the case in legacy security systems.

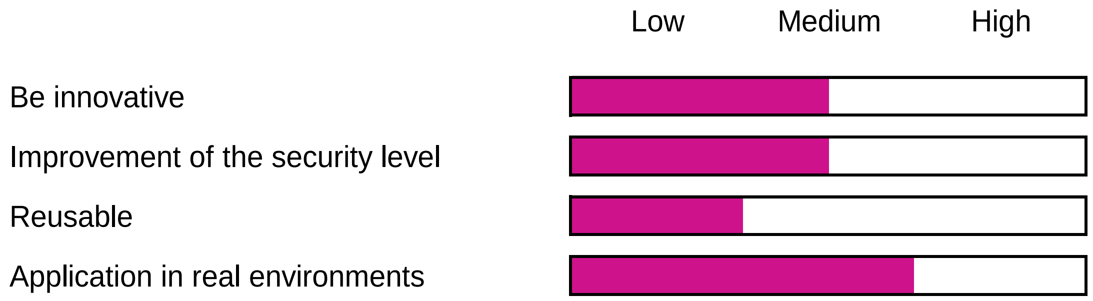
  As the capacity is a software running on a server in a technical room, there is no physical constraint in its use. However, as with other automated security procedures, the main open question is its suitability in the case of exceptional security events, which, by definition, are never twice the same.

Application in real environments

This capacity does not have any legal or regulatory constraint limiting the use of the capacity in any EU country. In addition, there is no concern about its acceptability in the general public, neither ethical concern or debate related to the capacity.

As a side positive effect, the capacity can be used to improve almost any system involved in the PT network. For example to orchestrate a physical assets supervision system (SCADA) with a maintenance management system, or to orchestrate traffic management systems with crowd management systems, adding more vehicles to journeys that have exceptionally high numbers of passengers.

On the other hand, its effectiveness may be reduced due to the difficult of the OCC operators to define, by themselves, new automated rules, as well as, the complexity of the configuration of such system could be a difficult added for applying in real environments.



4.2 Cyber security

Short description

Cyber security is information security as applied to computers and computer networks. The field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. Computer security also includes protection from unplanned events and natural disasters. In the framework of SECUR-ED, cyber security covers the following topics:

1. Best practice and preventive measures (cyber security risk assessment model, information systems backup and restore and user access for IT systems).
2. Detection and prevention (anti-virus/malware management, intrusion detection system for PTO operations).
3. Incident response (mitigation/restoration and IT vulnerability remediation management).

Conclusions

Be innovative

Although cyber security is a capacity widely used in other areas, it has not been used to the same extent so far in public transport areas. Within the framework of SECUR-

ED, a series of procedures have been established to cover the topics detailed in the description. A Risk Assessment guideline (based on ISO/IEC 27005) was produced for PTO operations. On the technology side, a cyber-intrusion detection system that applies an innovative approach to detect new attacks was specifically implemented for PTOs and demonstrated at Lisbon.

- **Improvement of the security level**

The technologies developed related to cyber security cover a wide range of areas (from monitoring to post analysis of possible incidents). This implies the use of some new technologies that were not previously used in public transport environments which is a great innovation regarding previous cyber security measures.

Improvement of the security level is not guaranteed in case a system does not work properly, so maintenance should be a key factor in a cyber security system. In addition, specially trained staff is required to take advantage of all the possibilities that a cyber security system may offer.

However, one of the “first-of-all” recommendations to prevent cyber-criminality is to enhance the physical security of the system like the access control in the technical premises.

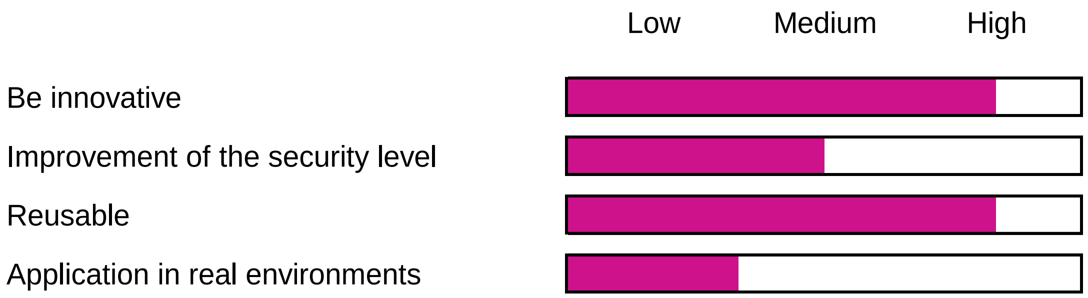
- **Be reusable**

Cyber security systems are easily reusable due to the ease of implementing IT systems in all kind of environments. However, it is essential to know the special features of the scenarios to adapt the systems properly.

- **Application in real environments**

At first, cyber security systems do not have important legal, ethical or acceptability constraints that may impede their application in real environments. However, as previously said, specific staff and maintenance are essential in all cyber security systems, so these costs have to be added to an initial investment.

Cyber security systems offer advantages that could not be provided without IT means. However these technologies have to be used integrated with physical security in order to cover all possible risks. Not separating physical and cyber security any more (from risk assessment by organizations and implementations) is also a point highlighted during SECUR-ED.



Future fields of research

During the development of the project it has been discovered that one of the major risks for PTOs in the future inside cyber security is the cyber-criminality. It would be necessary to intensify the research on this particular topic.

For most of the operators cyber-security is a more relevant concern each day. It should be taken into account at all level of organization and procedures.

4.3 CBRNe Sensors

Short description

CBRNe sensors are protective measures used in situations in which any of these four hazards (Chemical, biological, radiological and nuclear) are potentially present. To account for devices also involving explosives, the term CBRNe (e for explosives) is used. The sensor is a converter that measures a physical quantity and converts it into a signal which can alert to the security staff.

Conclusions

➔ **Be innovative**

The use of CRBNe sensors is innovative due to the capacity for detection, in one or various devices, of a large range of substances that may be involved in a chemical, biological, radiological, nuclear or explosive attack. In all these scenarios, due to their high potential impact, the possibility of detecting the threat and implementing an immediate response is essential in order to mitigate the adverse circumstances that arise from these attacks.

➔ **Improvement of the security level**

Although a CRBNe threat is a very unlikely risk, compared with the threats that PTOs face daily, these sensors may be key equipment at locations where a CRBNe attack may be expected. As said before, the potential for casualties and damage of this kind of attack is enormous and an early detection of the threat may be the only possible solution to mitigate the casualties and damage.

➔ **Be reusable**

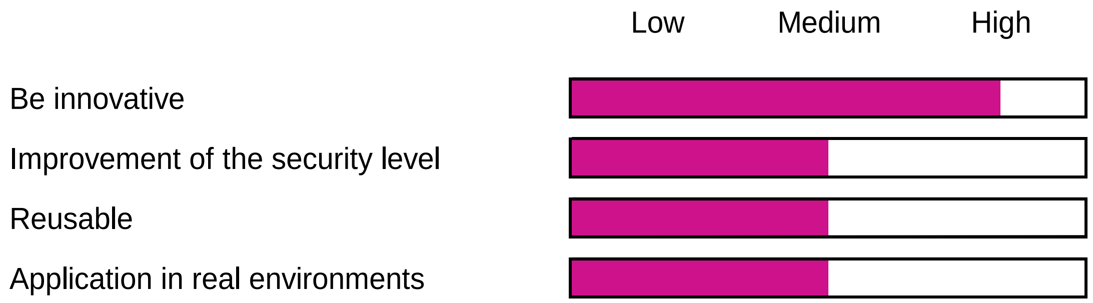
Specially trained staff is necessary to implement these measures properly due to the complexity of the operating principle which requires a correct installation of the devices and a correct reading of the measures. However, as in the case of other types of sensors (fire, smoke...) there are no further constraints in the wide use of these devices.

➔ **Application on real environments**

The use of CRBNe sensors is widely limited by the necessity of using toxic substance in order to compare the samples. This fact turns into legal, ethical and acceptance constraints.

Some sensors require a waiting time in order to take measures which lead to delays that are not accepted by the users and make the devices unacceptable in scenarios in which CRBNe risks are not clearly expected. On occasions, possible delays are avoided by taking only random samples or by using the devices only when CRBNe attack is imminent. As this knowledge is unlikely this approach decreases the effectiveness of the sensors. However the sensors selected as SECUR-ED module do not require an unacceptable waiting time (in D34.1 partners addressed this problem and found acceptable solutions)

Other factor that must to be taken into account is that the cost of CBRNE sensors is a major concern to allow deployment in any operator network



4.4 Tracking

Short description

Semi-automatic tracking is a tool provided to the CCTV operators to support them in doing more efficiently a task intensively performed today manually, after appropriate training.

This function, closely linked to video patrolling, may be activated locally for benign events as local regulations allow, but can also be run at the network security centre in real-time in case of more complex situations by authorized staff or more generally by the police; it can also be used post event by police to help in selecting the appropriate video sections requested by justice for forensics investigations.

On a case-by-case basis, the tracking results may accordingly be archived with the associated videos as dynamic metadata for reuse. Data and access protection in force for CCTV directly applies, always according to local policies.

Two modes of operations are considered. The first and main one (live analysis) deals with videos directly provided by cameras and the second one (post-analysis) deals with previously recorded videos.

After the user has designated a suspect individual (hereunder referred as “the target”) and a temporal way of tracking (backward or forward), the system tracks the individual over the video streams in which he/she is visible. At any given time, the system will provide the user with the next relevant video and the most likely target positions. At any time, the system also allows the user to confirm or select another proposal.

Advantages and answers to indirect needs for operators

- ➜ Enhancement of forensics and real-time intervention thanks to video-analytics and tracking tools.

Conclusions

➜ **Be innovative**

The innovation of the tracking systems developed in the framework of SECUR-ED is very high. These systems are able to track a person along the whole transport network combining different tracking methods as CCTV, face identification, Bluetooth, WIFI, RFID, etc. Regarding traditional tracking systems, this method is a huge innovation.

➜ **Improvement of the security level**

The improvement of the security level due to the use of tracking systems is very high. It allows appropriate measures following detection of all types of suspicious behaviours and location of the target person in a specific point within the transport network.

This system is an efficient support to prevent altercations or possible terrorist attacks against the transport network. This tool can also be used to track people in order to ease their arrest after crimes as graffiti, pick pocketing or robberies have been committed.

Finally, tracking systems are also an essential tool in most investigation cases due to the huge amount of information that they can provide.

➜ **Reusable**

The extensive use of the tracking in the different demonstrations and its ability to interface with dedicated IP based modern CCTV systems, but also with a variety of legacy digital or analogue CCTV assets, prove that it is easily adaptable to different infrastructures and scenarios.

As tracking is normally performed by a limited number of operators simultaneously in a given PT network, processing power (and associated computing costs) is limited to the few video streams (less than ten per operator) which can come from any camera of the network. Each camera, to be usable, needs naturally to have been calibrated with the system, but this process has been automatized within SECUR-ED and the job can now be performed remotely in less than 20 minutes per camera.

Tracking is normally performed intensively by police only; as allowed per local regulations, tracking may nevertheless be used by PT security staff in their routine activities.

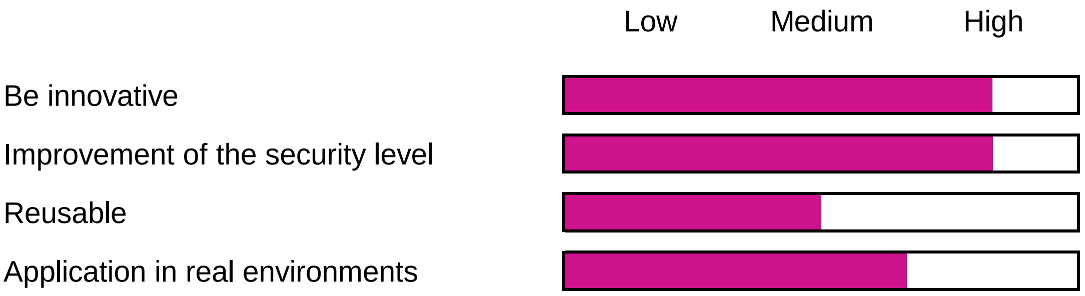
➜ **Application on real environments**

The application of tracking systems on real environments are not a big deal in the sense that they are adding a support in their normal duty to operators already trained to perform video patrolling; it is very instinctive and does not require more than a couple of hours of training.

As indicated above, the investment is limited, as few streams are activated simultaneously, and does not require changes to legacy CCTV assets, but only a future-proof interfacing to generate IP streams.

Technical constraints in terms of CPU processing and bandwidth still to be achieved in the future to ensure quality of service can be a hindrance for big networks tracking.

Pending local regulations and habits, tracking systems may imply ethical constraints if performed by PT staff (even if this task is done routinely today manually). This point disappears if tracking is performed by police.



4.5 Training

Short description

Training is the acquisition of knowledge, skills and competencies as a result of the teaching of vocational or practical skills and knowledge that relate to specific useful competencies. The training capacities developed during the SECUR-ED project may be classified as follows:

1. Training courses :
    a. Security training course for front-line employees
    b. Security awareness course for passengers
    c. Security CBT course for front-line employees
    d. Security training course for security agents
    e. Security refresher CBT course for security agents
    f. Security training course for operators in security command and control centres
    g. Simulator training for operators of CCTV system in the security control room
    h. Security training course for security managers
2. Exercises:
    a. Emergency and Crisis Preparedness Training Programme: focused exercise
    b. Emergency and Crisis Preparedness Training Programme: full-scale exercise

Advantages and answers to indirect needs for operators

➜ Increase the staff competences in handling security issues thanks to training lessons

Conclusions

➜ **Be innovative**

In general, training is a very mature capacity that has been used for decades in most environments. However, this is the first time a comprehensive batch of training courses specific to public transport security for general utilisation has been produced. Before use, adaptation to an operator’s particular circumstances is necessary, including, if necessary, translation. Training courses and emergency and crisis preparedness training is already widely used by larger, more experienced PTOs but it is less common, and especially important, for smaller PTOs. Some more innovative Computer Based Training sessions have been developed and reveal to be of great interest for PTOs.

➔ **Improvement of the security level**

The training courses have very broad uses as they deal with a variety of daily as well as terror threats. The topics of the developed training lessons range from preventive aspects to the management of security incidents. They target front-line employees (e.g. drivers of vehicles, in-vehicle service staff, ticket inspectors, station service staff, cleaning staff), security staff (e.g. in-house security staff, security services provider's staff), operators of security control rooms and security managers. In addition, lessons for different groups of passengers (kids, teenagers, adults) are developed. The lessons have broad uses; with some of them are also interesting for training non-urban transport providers or stakeholders that are not providing transportation.

The developed table-top exercises confront multidisciplinary teams of responsible stakeholders with emergency and crisis situations at both tactical and strategic levels and train correct communication as well as efficient decision making. The capacity/document itself provides guidance on organising exercises of many types and size. Therefore, it could be used for designing trainings for various threats and also broad uses outside urban mass transport security.

It is well known that training enhances the competencies of the staff. In order to achieve long-term effects, regular re-training is suggested.

➔ **Reusable**

Training courses are very easy to be applied in different modes of transport and in cities of different sizes. However, work is necessary to adjust the generic lessons, including translation, together with an appropriate internal or external trainer. Nevertheless, adjustments could be more challenging for some countries/cities because of national particularities (e.g. concerning the legal status and authority of security staff in PT networks).

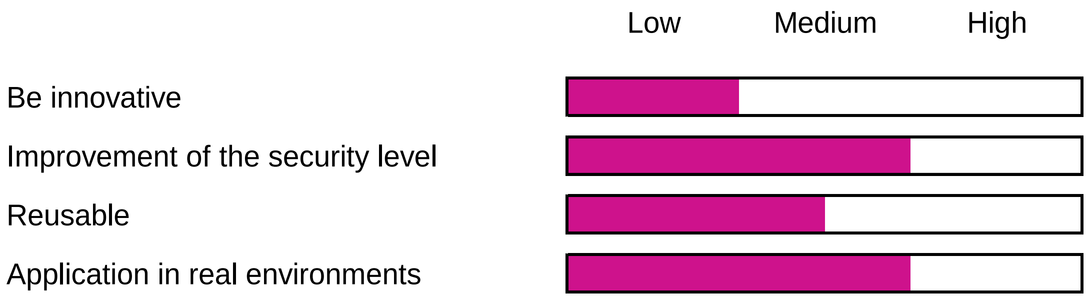
Emergency and crisis preparedness training is also very easy to be adapted to different scenarios but normally significant effort is required for planning exercises (e.g. logistics, cooperation with other stakeholders).

➔ **Application on real environments**

Normally, there are no legal constraints for delivering training to staff and passengers. Nevertheless, labour representatives and unions should be involved early in the process, in order to increase acceptance. During the planning of emergency and crisis preparedness trainings, legal and regulatory constraints have to be taken into account (e.g. to ensure the health and safety of all involved persons). Nevertheless, there are no general constraints.

In general, the general public appreciates well trained and professionally acting staff.

Nevertheless, the training courses have to take into account ethical considerations (e.g. the lesson on identifying and handling persons based on suspicious behaviour, appearance & findings).



4.6 Contribution to standardization

A security standard is a document established by international consensus and promulgated by an independent body, in response to a recognized need of harmonization or interoperability to improve security. It is usually a formal document that establishes uniform criteria, procedures or methods.

Standardization has a series of advantages as improving performance, reducing risks, encouraging innovation, becoming more sustainable and saving costs.

- **Be innovative**

  By essence, the objective of standardization is not to be innovative, but to improve overall efficiency of the security stakeholders in their usage of the best available solutions and procedures. It is accordingly an enabling tool for the solutions evaluated in SECUR-ED.

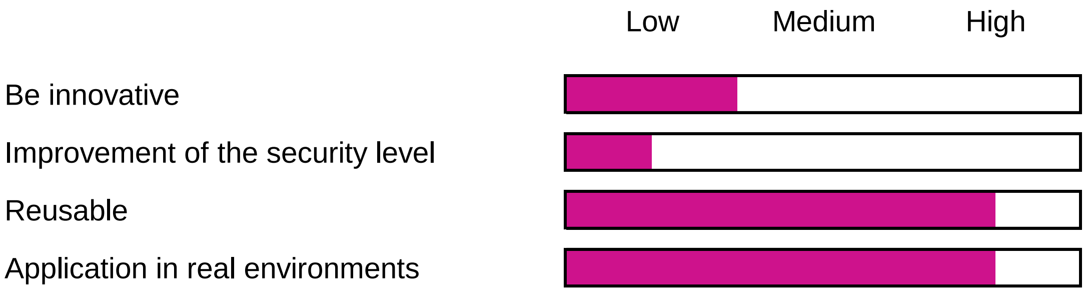
- **Improvement of the security level**
- Standardization aims at easing the implementation of solutions in different environments. Contributing to standards on security systems will then allow more security systems to be set up quickly so indirectly it will improve security Public Transport domain.**Reusable**

  Although standards improve performance of security systems, they must be general enough to be applied in all possible environments. This is why standards must concentrate on minimum requirements to achieve their objectives and leave freedom to the implementers to optimize the other aspects. This vision is supported by a recent EC mandate (M487) defining roadmap on security standardization in Europe.

  Reusability is a basic requirement of any international standard; the main pitfall to avoid is implementation of so-called “de-facto” or “industry” standards, proving not to be future-proof.

- **Application in real environments**

As for the previous point, standards are developed to be directly used in real environments, and therefore application in real environments is also an intrinsic characteristic in all standards.



Low
Medium
High
Be innovative
Improvement of the security level
Reusable
Application in real environments

5 Conclusion

This document intends to gather those practices considered as the best on a conceptual point of view. This remains preliminary and partly theoretical because it has been carried out before all the demonstrations. This document refers not only to technologies but also procedures, methodologies and those practices that SP leaders consider essential in the framework of the project.

Due to the huge amount of Capacities studied and analysed during the project, the most representative solutions of each demonstration have been chosen in order to cover as much material as possible. General methodologies and practices that SECUR-ED has intended to establish as essential in security analysis and design have also been included as best practices.

Practices selected comprise from those related to methodologies –standardization- to those related to technical aspects -cyber security and orchestration engine- including those related to human factors -training- or analytics in support to decisions - CRBN sensors and tracking.

This document is a first view of best practices foreseen in SECUR-ED project.

Other documents will be issued allowing further conclusions, among which the followings:

- Consolidation of the functional, operational and industrial results of the demonstrations
- Consolidation of the interoperability level achieved
- Consolidation of social and ethical impacts
- Recommendations to develop a risk reduction system
- Security plan deployment handbook
- Capacity & integration deployment handbook

The objectives will be dual:

- Identify/detail the ways of implementation of these best practices in the different topologies of public transport organizations
- Identify recommendations and new fields of experimentation for concepts that have been initiated within SECUR-ED.

6 Annex I SECUR-ED Capacities

Topic	SECUR-ED Deliverable	Flagship demonstration	Capacity ID no.	Capacities
Information Management	D35.1	Paris	INFO-01-01	Supervision Server
		Milan	INFO-01-02	Supervision Server
		Madrid	INFO-01-03	Supervision Server
		Paris	INFO-01-04	Supervision Server
			INFO-01-05	Supervision Server
			INFO-02-01	Orchestration engine
			INFO-02-02	Orchestration engine
		Madrid, Paris	INFO-02-03	Orchestration engine
			INFO-02-04	Orchestration engine
			INFO-02-05	Orchestration engine
	D35.2	Madrid	INFO-04	Passenger Information
		Madrid	INFO-05	Passenger Information System and Public Address
	D35.3		INFO-03-01	Post-event analysis (situation replay)
		Paris	INFO-03-02	Post-event analysis (CCTV forensics)
			INFO-03-03	Post-event analysis (CCTV and Incident)
Decision Support System	D36.5	Paris	INFO-06	Decision Support System - Early Warning System
	D37.3	Paris	INFO-07	Decision Support System - Restoration of Operations
Telecom	D35.5	Milan	TELECOM-01-01	Communication between vehicles and ground/wayside - via 3G/LTE/WIFI
			TELECOM-01-02	Communication between vehicles and ground/wayside - via 3G/LTE/WIFI

		Paris	TELECOM-02	Communication between field security staff and SOCC
			TELECOM-03	RFID ticket tracking
Video Related Analysis and Detection	**D33.3**	Madrid, Paris, Milan	CCTV-01-01	Fixed basic CCTV
		Paris	CCTV-01-02	Rail-standard basic CCTV
		Madrid, Paris	CCTV-01-03	Road vehicles onboard Basic CCTV
		Milan, Berlin	CCTV-01-04	Fixed basic CCTV
		Milan, Berlin	CCTV-01-05	Fixed basic CCTV
			CCTV-01-06	Fixed basic CCTV
		Milan, Berlin	CCTV-02-01	Wayside - Detection of persons in indoor areas supposed to be empty
		Milan	CCTV-02-02	On-board Empty Vehicle Detection (OEVD)
			CCTV-02-04	Wayside - Perimeter anti-intrusion and graffiti prevention
		Madrid, Paris, Milan	CCTV-04	Person tracking in video
			-	Person tracking in video
		Milan	CCTV-05	Wayside - Crowd abnormal behavior detection
			CCTV-06-01	Crowd Density Detection - On-board
		Milan	CCTV-06-02	Crowd Density Detection - Wayside / Fixed Facilities
		Paris	CCTV-07	Face recognition
				Unattended object detection
	-			Unattended object detection
CBRN-E	**D34.2**	Milan	CBRNE-01-01	Chemical & Explosives Detection - RAID-S2 (Bruker) IMS Sensor System
		Paris	CBRNE-01-	Chemical Detection - AP4C

			02	
		Paris	CBRNE-01-03	Chemical & Explosives Detection - Street Lab Mobile (TICs/TIMs, explosives, narcotics, and CWAs)
			CBRNE-01-04	Chemical & Explosives Detection - SAWEX (Vapor detection system using Surface Acoustic Waves technology))
		Paris	CBRNE-01-05	Radiological Detection - GAMPIX (gamma imaging system)
		Paris, Milan	CBRNE-01-06	Radiological Detection - DIRAD (automatic gamma detection system)
		Paris	CBRNE-01-07	Radiological Detection - Smart Gamma Probe (Area Monitoring and Alarm Triggering)
		Paris	CBRNE-01-08	Radiological Detection - CZT Handled Spectrometer (Miniature spectrometer)
			CBRNE-01-09	Radiological Detection - Portal Monitor (detect radioactive source in vehicle with a 15km/h max speed)
		Paris	CBRNE-01-10	Explosives Detection - T-REX (Portable vapordetection system)
			CBRNE-01-11	Explosives Detection - FLUODEX (nitro-aromatic explosives vapor detection - Fluorescence technology)
		Paris	CBRNE-01-12	Explosives Detection - SYPODEX (Vapor detection using Quartz Crystal Microbalance technology)
		Paris	CBRNE-01-13	Explosives Detection - QCL Portal PBIEDs (Personal Borne Improvised Explosive Device) Detection System
		Paris	CBRNE-01-14	Explosives Detection - Mobile Trace Portable Narcotics and Explosives Detector

Cyber Security	**D35.4**	Paris	CYBER-01-01	Good practice & preventive measures - Cyber security risk assessment model
		Paris	CYBER-01-02	Good practice & preventive measures - Information Systems Backup & Restore (procedure)
			CYBER-01-03	Good practice & preventive measures - User access for IT systems (procedure)
			CYBER-02-01	Detection & Prevention - Anti-Virus / Malware Management (procedure)
			CYBER-02-02	Detection & Prevention - Intrusion Detection System for PTO operations
		Paris	CYBER-03-01	Incident response (mitigation/restoration) - IT Vulnerability Remediation Management (procedure)
Training	**D38.1, D38.2**	Berlin	TRAINING-01	Security training course for front-line employees
			TRAINING-02	Security awareness course for heterogeneous groups of passengers
			TRAINING-03	Security CBTComputer based training (Computer based trainingCBT) for recurrent awareness training of front line employees
	D38.1, D38.3	Berlin	TRAINING-04	Security training course for security agents
			TRAINING-05	Security refresher CBT course for security agents; including a computer based training (CBT) module
	D38.1, D38.4	Berlin	TRAINING-06	Security training course for OCC operators in security command and control centres
		Berlin	TRAINING-07	Simulator training for operators of CCTV system in the security control room
	D38.1,	Berlin	TRAINING-	Security training course for security

	D38.5		08	managers
	D38.1, D38.6	Berlin	TRAINING-09	Emergency and Crisis Preparedness Training Programme: Focused exercise
		Berlin	TRAINING-10	Emergency and Crisis Preparedness Training Programme: Full-scale exercise
Depot Protection	**D32.3**	Milan	CCTV-02-03	Wayside - Perimeter anti-intrusion and graffiti prevention for Depot Protection and infrastructure protection
			ADD-01	Biometric for access control
			ADD-02	Paint Sniffer
Preparedness	**D31.1, D31.3**	Madrid, Paris, Berlin	ADD-05	Organisational, operational and IT procedures & plans
	D31.1, D31.3	Madrid	ADD-06	Incident response plan
	D31.2		ADD-03	Best practices for conducting risks assessments
	D31.4		ADD-04	Risk analysis software
Simulation	**D23.3**			Agent dispersion
	D23.3	Milan	SIMU-01	Evacuation modelling

- End of Document-