SECured URban transportation - European Demonstration

D46.5 REPORT ON CONSOLIDATION OF INDUSTRIAL RESULTS

Document identification			
Related SP / WP	SP4 / WP46	**Reference**	SCR-WP46-D-ANS-007
Related Deliverable	D46.2-6	**Dissemination Level**	PU
Lead Participant	Ansaldo STS	**Lead Author**	Ansaldo STS
Contributors	ICCA, ALSTOM, ANSALDO, ATM, CTRM, DB, FNM, RATP, THALES	**Reviewers**	PMB

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

History

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

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

Version	Status	Date	Author	Main Changes
1.0	Draft	16.05.2014	ASTS	Initial draft
2.0	Under review	16.09.2014	ASTS	Contribution from Thales and internal revision
2.1	Under review	29.09.2014	ASTS	Review comments from RATP, BT and MTRS3
3.0	Issued	30.09.2014	THALES	Version sent to the Commission

TABLE OF CONTENTS

1 Abstract & Purpose

1.1 Abstract

This document is a systematic collection of information and results of the four flagship demonstrations.

The collection of demonstrations served to illustrate the eminent security needs of Public Transport Operators across Europe; and the maturity of modern technologies and design that supports harmonized migration from legacy systems.

This document is focused on industrial security benefits of the demonstrations and the consequent industrial impacts. The stakeholders to each of the security threats addressed out of SECUR-ED contributed to the evaluation of the capacities demonstrated. Conclusions and pragmatic recommendations on industrial subject matters based on the results of the four flagship demonstrations are highlighted through this document.

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

1.2 Purpose of the document

The purpose of this document is to report on industrial impacts noted from the four flagship demonstrations. The report reflects the results of the inputs of the involved operators and integrators. This includes a summary of the results from the questionnaires completed after each demonstration; which takes into account the respective capacities demonstrated, as well as the specific security objectives, situational/operational, and environmental conditions.

The objective is to highlight how the security of mass transportation systems can be enhanced and sustained using the technologies and best practices demonstrated out of SECUR-ED.

In accordance to the original SECUR-ED project approach, each demonstration complied with the general architecture, and had its own respective design to adapt to local requirements for the integration of capacities. This document represents a summary and high level assessment of the project results surrounding the four flagship demonstrations; including descriptions on the differences in administration, business, and operational points of views.

1.3 Structure of the document

The document is structured into 5 sections as follows:

- Abstract & purpose (current section)
- References: acronyms and referenced documents
- Rationale and methodology
- Industrial results
- Conclusions.

2 References

2.1 List of acronyms

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

2.2 Referenced documents

The following documents are referenced:

R[1]	COUNTERACT / PT5 - Public transport security planning - organisation, countermeasures & operations guidance. Available at http://www.uitp.org/knowledge/projects-details.cfm?id=433
R[2]	SECUR-ED D21.1 - Public Transport Security Terms & Definitions
R[3]	SECUR-ED D21.3 - Overall Approach to Security Management and Emergency Preparedness
R[4]	SECUR-ED D51.2 - Experimentation Building Manual
R[5]	Transit agency security and emergency management protective measures, Federal Transit Administration (FTA), November 2006
R[6]	Transit Security Design Considerations, Federal Transit Administration (FTA), November 2004
R[7]	Technical Recommended Practice for the Selection of Cameras, Digital Recording Systems, Digital High-Speed Networks and Train-lines for Use in New Transit-Related CCTV Systems, APTA Technical Standards document, August 2008
R[8]	MODSafe Modular Urban Transport Safety and Security Analysis, Deliverable No. D 9.1 - Hazard scenarios related to security aspects
R[9]	Institute for Security & Open Methodologies www.isecom.org
R[10]	Physical Security Information Management www.psimtrends.com
R[11]	An introduction to video content analysis industry guide, British Security Industry Association, June 2009
R[12]	Railway industry website www.railway-technology.com
R[13]	ISO 31000, Risk Management Standard
R[14]	SECUR-ED D4x.1.- Detailed scenarios for demos
R[15]	SECUR-ED D4x.2 - Functional specifications for demos
R[16]	SECUR-ED D4x.5 - Consolidated results for Milan, Paris, Berlin and Madrid demonstrations
R[17]	SECUR-ED D46.1 - Guideline for Results Consolidation
R[18]	SECUR-ED D33.1 - Report on Video Analytics enhanced
R[19]	SECUR-ED D35.5 - Telecommunications

3 Rationale & methodology

In SECUR-ED, several capacities, tools, techniques and procedures have been integrated and demonstrated during the development of the four demonstrators in order to enhance transportation security management. SECUR-ED has investigated different scenarios in different cities, offering multiplicity aspects and factors that make up security in transportation systems whilst mediating among many needs, constrains and economical evaluations; it also involved actors wishes for sure.

Security systems are "sensing systems", which are at the heart of a high-growth market. But they are also very strategy-intensive and, as such, they create important economic, social, organizational and environmental challenges for operators. SECUR-ED through the collaborative initiative of a multi-disciplinary team, and by pooling know-how from researchers, academics, manufacturers and operators, has managed to stimulate, at the very heart of a cutting-edge issue, continuous improvement dynamics for transportation systems.

SECUR-ED project answered to many challenges inherent to security for transportation system. In this way SECUR-ED has had many operative plans to improve the security from technological consolidation to definition of interoperable requirements, from trying to define interfaces and integration criteria to guarantee modularity for any kind of capacity differing for age and technology, defining a simple, versatile and flexible security framework reusable in most contexts in accordance to local ethical issues.

The spirit of the project was to stimulate the integrators to assemble, integrate and interface the majority of available technologies including legacy systems, proprietary subsystems, off-the-shelf and dedicated technologies. For this purpose the architecture of the project includes a Subproject (SP3) focused on capacities Integration.

Since the implemented scenarios were heterogeneous in the technologies involved, in the objectives to be reached and in the application context, the collected data are not easy to aggregate and harmonize.

According to Guideline for Results Consolidation, the present document is the outcome of Task 46.5 and it collects the evaluation of SECUR-ED industrial impacts by operators and integrators.

As indicated in these guidelines, the scope of the document is focusing on:

- the level of maturity of technologies applied and tested in the different demonstrations;
- the degree of industrialization achieved and the necessary effort needed to arrive to an industrial product;
- the competitiveness of the demonstrated solutions, relative to existing or other methods / systems responding to similar functions;
- the complexity of the demonstrated solutions, especially in terms of integration to legacy equipment, systems and procedures;
- the investment, operational and life cycle cost of the demonstrated solutions;
- the resilience of proposed solutions.

The above topics have been analyzed at the end of each demonstration. The collection of all these aspects is an input to identify a set of indicators to estimate costs/benefits ratio of fulfilment of the security needs/improvements. This information is strategic to evaluate reusability of SECUR-ED results and choices in other public transport systems than those in which they have been demonstrated.

The objective of the document is to put in a common frame, the individual local experiences of each demos, in order to capitalize on, in respect of each strategic and economic characteristics, the elements of success of the proposed security solutions and minimize both risks and technological gaps among different technologies and practices. The identification of common elements and similar procedures may also produce the definition of shared tools, able to minimize the costs and encourage the reuse and integration of already available technologies, in the spirit of a necessary improvement of the use of available resources.

The aforementioned items have been investigated with the aim to respond to the guidelines sketched in D46.1 where applicable in relation to the specific characteristics of each scenario.

The table below summarizes the capacities involved in each demonstrator.

Functionalities \ Demo	Madrid	Milan	Paris	Berlin
Telecommunications systems	X	X	X	
CCTV systems	X	X	X	X
Video Analysis		X	X	
CBRNE systems		X	X	
Cyber technology			X	
RFID		X		
Localization Technology	X		X	X
Emergency procedures	X	X	X	X
Integrated Information Management Tools	X	X	X	X
Operator training & simulation		X		X

4 Industrial Results

4.1 Level of maturity of technologies

The following sections report some evaluations on the level of technological maturity of capacities applied and tested in the different demonstrations.

4.1.1 Integrated Information Management Tools

Overall, the Information Management tools have shown a good level of maturity. They are able to integrate multiple and different legacy and/or new physical security systems and subsystems into one common operating paradigm. Thanks to use of standard interfaces, any kind of subsystem can be easily integrated. They are able to manage and control several devices while automatic warnings mechanism increases the operators' trust in the system. Through the events operators are immediately aware of the situation and the reaction time decreases. Furthermore, some of these tested implementations allow insertion of standard operating procedures to be used in an emergency situation.

Recommendation(s):

- Solidify the results obtained through an international standardization of a minimum set of events metadata (consistently with Mandate 487 recommendations).

4.1.2 Telecommunication systems

The telecommunication systems are in a mature phase by now thanks also to the massive introduction of digital communication technologies. They provide a wide range of scalable and reliable solutions which fits well the transportation environment. Over the past few years, PTO's have shown interest in evolving technologies and willing to move away from legacy system to more sophisticated commercial and private technologies, like cellular network, Wi-Fi, WiMAX etc. The trend goes towards the adoption of hybrid systems like integration of GSM-R with Wi-Fi and TETRA over LTE. Here the resilience is ensured by the legacy system and bandwidth requirement is fulfilled by latest wireless technologies like Wi-Fi, WiMAX, 3G and LTE. Some of these technologies require a purpose built network infrastructure (like Wi-Fi & WiMAX), in which some of them entirely rely on third party network infrastructure (like 3G & LTE). Due to the fact that telecommunication equipment becomes increasingly more affordable (this is specially the case with Wi-Fi), PTO's are willing to adopt these new technologies in the near future.

Recommendation(s):

- Train to wayside communication links form a crucial subsystem in delivering diversified public transport security and infotainment applications on-board. Delivering such a communication subsystem and fulfilling the QoS and resilience requirements of a broad range of applications is always going to be a challenge.
- Redundancy between commercial and private network can be achieved by increasing the end-to-end throughput by combining both networks when available.
- For real-time video streaming, a case-by-case trade-off between unicast and multicast must be made. While unicast may be beneficial when there is only one or few

consumers, multicast helps to preserve scarce bandwidth when there are multiple consumers scattered over different locations. Adaptive variable bit rate streaming could also be beneficial for preserving scarce bandwidth, but there is no mature solution yet due to a lack of standards.

4.1.3 CCTV Systems &Video Analysis

The level of maturity of CCTV systems is getting higher. They are commonly used by most PTOs and well used within all networks of various cities in which demos have been performed. Multimodal and Multi-PTO CCTV implementation for both fixed and on-board cameras has been performed for almost all PTOs and its performance is successful. On a technological point of view, digital video over IP still remains to be generalized on the networks (such large networks require several years before being able to complete a full change of technology generation). But all demos have demonstrated that it is possible to create interfaces with legacy CCTV tools.

Video analytics and intelligent video surveillance are very active fields of research and they have a wide spectrum of promising security applications for both indoor and outdoor. The SECUR-ED project has tested some of these (tracking tools, crowd detection, intrusion detection for perimeter protection and on board empty detection) examining the practical issues of video technology application in relation to the context of public transportation. In particular, factors as real-time capabilities of systems, environmental conditions (including architecture of existing infrastructures) and hardware resources have to be considered. Furthermore the system calibration has a critical role, as the application software has to be adapted on the supervised scene and be adjustable to new conditions. Taking this into account and on the basis of experiences gained from four demos, we can affirm that:

- Tracking tools are almost industrial solutions, but success in this topic doesn’t only rely on the solution itself, it needs also a high quality level of cameras and data transmission, relevant angles of filming, good lightning and appropriate maintenance. In particular,
  - for *semi-automatic tracking* some attention and development points are on the automatic re-identification of the person between one camera to another and small ergonomic adjustments on the target designation are under progress.
  - facial recognition is one of the few video analytics tool not requiring camera per camera calibration.
- Intrusion detection for perimeter protection has a high level of technology maturity and is a robust solution.
- For crowd detection, some enhancements have been done but still needs some improvement work. Commercial products for crowd detection and overcrowding in outdoor areas are expected in the near future.
- On-board empty detection has a good level of technology maturity.

Recommendations:

- Design the CCTV systems architecture in a modular way; i.e. properly separating the basic functions in such a way that the ONVIF (IEC 62676-1&2) principles are implemented and subsystems of different vendors can easily be added to an existing configuration.

- A generalised use of RTP/RTSP streams carrying video H264 compressed metadata time stamped at the frame level is recommended.
- Video-surveillance systems are nowadays networks of distributed PC's; as such they are potential targets of cyber-attacks, against which they must be protected (physically, by training staff and with software).
- Digital video, especially when live information with low latency is required, has stringent needs for communications channels (no buffering is allowed); this implies a good quality of service for the communication but also an optimised set-up in the network architecture to minimise throughput at any point of the network in all circumstances (typically a case-by-case trade-off between unicast and multicast).

4.1.4 CBRNE systems

Nowadays industries have prepared and demonstrated relevant sensors for hazardous material detection. Furthermore the market standard products are not specific to the transportation systems and the need for regular calibration is probably an issue because only simulative tools are used since real tests are not possible.

Note(s):

- Market remains limited by the fact that it *is not* -so far- in its normal duties for a PTO to deal with CBRNE threats. Would that change ever, open coordination with relevant authorities would be needed on a daily basis, and organisational changes would take place, including extra staff, as well.
- Generally speaking, the current solutions for CBRNE passengers scanning are not directly suitable for application in urban transportation due to their excessive processing time not compatible with crowd flows, but can be used e.g. in combination with canine patrols, probably over a fraction of the flow.

4.1.5 Cyber security technologies

It is a set of emerging methods and solutions for PTOs and the first step was to prepare the organizations to take on this new challenge. Efficient and reliable solutions are available to address a wide range of needs.

Recommendation(s):

- Cyber security is of growing importance for the public transport sector. The public transport industry needs to establish security standards and best practices for information security management like the ISO 27000 series. In this context security technologies would be needed, like VPN for secure collaboration in distributed locations, MPLS for high-performance routing in large networks, redundant network connections in case of a failure or an attack, virtual LANs for a secure segregation to guarantee the required quality of service for safety applications.
- The public transport industries must acknowledge, as well, that information technologies have invaded all the functional modules, including the "physical" ones and

that the above prescriptions apply to a growing number of operational systems, which need to be specified accordingly.

- Above measures can be successful only with constant awareness campaigns towards the users involving not only technological tools but also best practices on human behaviour.

4.1.6 Localization Technology

The level of demonstrated localisation technologies is good when outdoor, insufficient when indoor or underground. When applied in surface transport, this technology is ready to manage incident for all PTOs in the whole region, but improvable to enhance response times and automatic decision taking.

Recommendation(s):

- Start to develop methods (and then standards) for underground infrastructures or inside buildings.

4.1.7 Operator Training, Emergency procedures & Simulation

The simulation is a mature technology for most of the considered solutions and - in particular - whenever real-field test are interfering with the daily PTO's operations. Its strength is its totally independence by operational activities, it can be used without interfering with the normal operations.

4.2 Degree of industrialization achieved

The process of industrialization of the initial phases of the project has produced as an outcome the definition of a project methodology in order to have an integrated architecture for improving the security of transportation systems. The four demos have demonstrated that, by means of a SOA approach combined with the use of standards, it is possible to develop a single interoperable urban transport security framework which can be applied to heterogeneous environments. The realized solution results in a flexible architecture that allows to integrate easily and regularly new capacities with limited effort whilst partly reducing the time for the deployment and the non-recurrent engineering costs without dictating any constraint about the implementation of applications. This is a key result in sectors such as transportation because it slows down the obsolescence of technologies whilst, at the same time, enabling innovation by adding new capacities.

4.3 Competitiveness of the solutions

The realized solutions have proved a successful strategy for improving security within the transportation environment since they define a methodological approach that describes "how" disparate security measures and technologies should be integrated and not simply "what" should be integrated. It is an highly competitive solution which allows, when developed at full operational level:

- To realize a relatively easy integration combining new capacities with the existing ones.
- To simplify and streamline the partners interactions despite a wide variety of technologies.
- To have a platform of agnostic paradigm (operating system, development environmental, programming language, hardware setup).
- To have a flexible architecture not specific to operator, or city, or country but applicable at any critical context after some regular setup.
- To use standard and free tools for testing procedures without dictating any constraint about the implementation of applications.

Note(s):

It is quite clear from the demonstrations that economic benefits generated by the adoption of integrated security solutions (e.g. reduction of thefts, reduced vandalisms, etc.) are not sufficient to justify their costs due to a series of causes, including intrinsic cost of technologies, not fully-reached maturity of some technologies, intrinsic size of the "problem" (e.g. kilometres of lines, number of stations), etc.

Security installations generate a positive cost and benefit ration only whenever non-tangible costs are included in the cost function:

- security perception;
- business continuity;
- operator's reputation;
- etc.

4.4 Complexity of the solution

Despite its complexity the solution is very attractive since it is an architectural style that enables the reuse of existing legacy assets within a new paradigm that facilitates reusability, abstraction of underlying logic, loose coupling, flexibility, and scalability allowing an evolution of technologies. In particular, we report the perceived complexity of the individual technologies in term of integration to legacy equipment, systems and procedures.

In the SECUR-ED project, one notable challenge common amongst the integration of most technologies on legacy systems has been picking vehicles / subsystems that are no longer in their warranty period to avoid potential voiding of active warranties.

4.4.1 Integrated Information Management Tools

These systems have different levels of complexity on the basis of provided functionalities. In particular, they deal with monitoring and management of events detected, real time interaction and decision support. Thanks to a Service Bus as integration strategy, it has been possible to integrate easily whichever physical security system is involved, taking advantage of standard interfaces and protocols.

Recommendation(s):

- It is important that the information management tools are designed in such a way that a “qualified human” remains in the loop with the best possible situational awareness. This means the deployment of tools that reduce the non-critical human interventions and allow concentration on the key activities for emergency preparedness, management and post event forensics.

4.4.2 Telecommunication systems

Most Operators are lacking a modern telecommunications system that would support the requirements of modern technologies that are available today and of the future. As a project focused on transportation, the primary focus on telecommunication was on supporting the communication between vehicles and ground/wayside to support security applications. The SECUR-ED work was extended to include more extensively the recommended practices in the assessment and adaptation of commercial-off-the-shelf telecommunications technologies to support the needs of an Operator. The following are some high level recommendations aligned with what has been elaborated in the project:

Recommendation(s):

Public transport operators should conduct a thorough site survey for integrating Telecom Capacities in a public transport environment and be wary of key considerations such as:

1. <u>Coverage</u>: certain telecommunication technologies being better adapted to specific transport network environments (long distances, underground tunnels, bridges and overpasses, etc.);
2. <u>Frequency limitations</u>: country or local regulations sometimes limiting the availability of certain frequency ranges (commercial telephony, military exclusive bands, etc.);
3. <u>Performance</u>: technological performance figures such as data rate and latency proving to be critical for certain systems or functions;

4. Maturity: standardized, enduring and mature technologies providing better long term investments;
5. Availability: the proportion of time the telecommunication system remains in a functioning condition dictating its potential use for specific operational functions;
6. Reliability: reliable communication equipment simplifying the life cycle management;
7. Maintainability: maximizing the telecommunication products' useful life;
8. Total Cost of Ownership: including the life cycle cost over many years of operation;
9. Quality of Service: Whenever CCTV video streams need to be transported, special attention shall be given to the quality of service (QoS) of the communications.

4.4.3 CCTV Systems &Video Analysis

The CCTV systems don't exhibit any complexity thanks to their high technological maturity level. They are widely used in critical contexts and represent important reference technologies for the security.

The video analysis systems have a certain degree of complexity which mainly lies in the decision on how to perform the analysis. The location of analysis becomes more and more important considering flexibility and reliability. In general there exist three modus operandi: inside the camera, cameras with integrated computer unit, or on external workstations. The decision on how to manage this depends on the required computing power, the size of the installation, and on the ability to be integrated in existing systems by interfaces. A central workstation can process several complex algorithms at the same time while the already existing cameras can still be used. The system is easily expendable, although the data have to be transferred to the analytic server: that requires high bandwidths. If the workstation fails, analyses are suspended. By contrast, decentralised analysis is less liable to breakdown. The maximum number of supported cameras can vary as well as the number of supported providers. In addition, further complexity elements are due to privacy aspects since not all countries have laws and regulations that authorize the use of video analysis algorithms.

4.4.4 CBRNE Systems

The technological evaluation of CBRNE systems is very complex because it involves different aspects not only of a political nature but concerns also priority setting and assessment of needs. The cost of this technology is rather high so it is essential to balance the security needs with budgetary constraints, and the protection of human rights with the individual freedom. For example when detectors are installed at entrance and exit points they slow down the free movement of people.

Note(s):

- One must be aware that tests in real operational conditions are very difficult to perform.

4.4.5 Cyber security technologies

Nowadays urban transport systems are heavily based on ICT tools to run daily operations, thus opening the door to cyberattacks.

The project has shown that there are mature technologies to protect PTO's ICT infrastructures from cyberattacks. However:

- the cyber criminality is continuously raising the challenge by introducing more and more sophisticated cyberattacks, thus increasing the complexity;
- the high level of heterogeneity of adopted ICT solutions does not allow to generate a generic cyber protection solution usable in all PTOs premises;
- the intrinsic interaction with safety systems poses serious problems when adopting cyber-protection solutions (e.g. the traditional operation of patching new antivirus into safety-critical ICT systems requires - in principles - a new safety certification of the system itself).

4.4.6 Localization Technology

The outdoor localisation (typically GPS) is a mature solution that is nowadays available in many sensors and devices and easily integrated in security system. The current complexity, not fully solved in SECUR-ED is the seamless localisation in both outdoor and indoor areas where no standardisation exists and indoor solutions are not yet sufficiently precise and reliable.

4.4.7 Operator Training, Emergency procedures & Simulation

The major complexity during the operator training is to find and develop relevant training scenarios in the PSIM system.

The complexity of simulation tools depends on the model. The more the model is faithful to reality the more the simulation is accurate. This requires a particular sensitivity and awareness during the model definition.

4.5 Investment, operational and life cycle costs

Adopting an SOA-based integration framework has had a clear impact on the investment, operational and life-cycle costs. In particular:

- it extends the life-cycle of the implemented solution by slowing down the need for the replacement and update of technologies since the modularity allows gradual adjustments whilst guaranteeing the service continuity;
- the seamless integration of new capacities with the existing ones allows maximizing the return on investment by reducing the non-recurrent engineering costs;
- the large adoption of standards and open tools reduces the cost of training - and in particular reduces the number of staff knowledge updates.

Recommendation(s):

- As life expectancy of systems building blocks may reach several decades, it is crucial that the key SECUR-ED prescriptions appear as soon as possible in the procurement specifications for new systems.

4.6 Resilience of solutions

The adopted solutions are - in general - able to mitigate the propagation of damages minimizing the disaster recovery in time and space in terms of contribution to the resilience of transport systems.

5 Conclusion

The project proved the composite nature of the security and has experienced as many factors, including intangibles ones, contribute to define effort, costs and potential for success.

Human interaction, social and geographical differences, law, different languages have been significant difficulties to face to reach the objective of real integration of technologies.

SECUR-ED demonstrated a spectrum of technologies on the market that are mature enough to address a large number of the security challenges faced by PTOs today. Furthermore, the project has demonstrated how the cooperation between communities of academics, industries, and operators can creatively collaborate and collectively derive valuable solutions that address the challenges of the industry.

The data available and the reported experiences are quite exhaustive to appreciate the characteristics of each subsystem in order to satisfy specific business, organizational and administrative need in four different local administrations and the transferability of solutions.

The activities of the demos were limited in time, therefore not allowing evaluation of many economical indexes which are relevant to analyse industrial impacts of adopted solutions. However each demonstration allowed to estimate industrial costs and implications of the implementation of security system to protect a transportation infrastructure, starting from personnel training to the need of higher cooperation among all the authorities and stakeholders involved in the any field of citizen protection.

The main industrial impact of the project is centred around the adopted Service Oriented Architecture (SOA) that promotes a modular design framework that eases the integration and compliance of technologies into the complex heterogeneous environments of public transport systems.

Finally it is worth noting that the overall SECUR-ED future-proof conclusions and recommendations are to be found in the D01.11 “SECUR-ED Final Report” and associated White Paper.

- End of document -