SECUR-ED
SECured URban transportation - European Demonstration

D46.4 REPORT ON CONSOLIDATION OF THE INTEROPERABILITY LEVEL ACHIEVED

Document identification	
Related SP / WP	SP4 / WP46
Related Deliverable	D46.2-6
Lead Participant	Ansaldo STS
Contributors	ICCA, ALSTOM, ANSALDO STS, ATM, CTRM, DB, FNM, RATP, THALES

Reference	SCR-WP46-D-ANS-004
Dissemination Level	PUBLIC
Lead Author	ASTS
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	23.07.2014	ASTS	Initial draft
1.1	Draft	31.07.2014	THALES	Comments
2.0	Draft	09.09.2014	ASTS	Review after comments
2.1	Draft	18.09.2014	ASTS	Review after comments
2.2	Draft	19.09.2014	Thales/ASTS	Thales and ASTS minor changes
2.3	Under Review	19.09.2014	ASTS	Final draft ready for review
2.4	Under Review	29.09.2014	ASTS	Review comments from RATP and MTRS3 inserted
3.0	Issued	30.09.2014	THALES	Version sent to the Commission

TABLE OF CONTENTS

1 Abstract & Purpose

1.1 Abstract

The document is a systematic collection of information, constraints and results about the level of interoperability reached by the demonstrators of SECUR-ED project.

According to the SECUR-ED aims, each demonstrator was a test-bed intended to demonstrate that it is possible to improve security in public transportation systems, to show the feasibility of harmonizing and integrating legacy systems, mature and/or COTS technologies. The document describes also choices, procedures and constraints faced in this analysis in order to guide future project.

This document assumes that the reader is familiar with the SECUR-ED project and the objectives and scenarios of the four main demonstrations (Madrid, Paris, Milan and Berlin).

1.2 Purpose of the document

The purpose of this document is to define parameters and indicators in order to evaluate the interoperability level achieved and to formalize the analysis results.

According to the objectives of WP46 and, in general, of the whole SECUR-ED project, the final aim of this document is to reach the definition of a set of parameters able to measure the interoperability level of IT systems for Public Urban Transport Security to:

- arrive to practical conclusions;
- extract conclusions relevant to future scenarios / situations / operations.

2 References

2.1 List of acronyms

COTS	Commercial Off-The-Shelf
EC	European Commission
EU	European Union
ICT	Information & Communication Technologies
IPR	Intellectual Property Rights
ISO	International Standards Organisation
LAN	Local Area Network
LRT	Light Rail Transit
LRV	Light Rail Vehicle
OCC	Operations Control Centre
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	State of the Art
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WP	Work Package

2.2 Referenced documents

The following documents are referenced:

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

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

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

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

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

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

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

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

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

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

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

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

R[13] ISO 31000, Risk Management Standard

R[14] SECUR-ED D4x.1 - Detailed scenarios for demos

R[15] SECUR-ED D4x.2.- Functional specifications for demos

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

R[17] SECUR-ED D46.2 - Consolidation of Functional Results

R[18] SECUR-ED D43.5 - Consolidated results for Paris demonstration

R[19] SECUR-ED D42.5 - Consolidated results for Madrid demonstration

R[20] SECUR-ED D44.5 - Consolidated results for Milan demonstration

R[21] SECUR-ED D45.5 - Consolidated results for Berlin demonstration

R[22] Annex-1 Demo Madrid Results

R[23] Annex-2 Demo Milan Results

R[24] SECUR-ED D22.1- Interoperability Concept

3 Rationale & Methodology

The aim of this section is to explain how SECUR-ED project reached the interoperability goals. The interoperability level achieved is first estimated and represented, starting from a general interoperability concept defined in R[24], and from the guideline defined in R[16].

In order to include several and different aspects, this analysis led to define two classes of interoperability:

- Technological Interoperability;
- Managing & Procedural Interoperability.

The first class, “Technological Interoperability”, includes all interoperability opinions expressed on technological issues. As technological issues, we mean all aspects that concern SW and HW implementation and integration. For example specific interoperability concepts are here included, such as technical, syntactic, semantic and pragmatic interoperability, as also more general concepts, such as the interoperability among SECUR-ED solutions, or new and legacy systems.

The second class, “Managing & Procedural Interoperability”, includes all aspects that concern the cooperation among several providers and operators, and in general among many different partners.

The following sections will explain more in detail how this analysis has been conducted, and how were collected and understood the feedbacks.

3.1 Technological Interoperability Class

The technological interoperability class is based on scientific aspects: indeed R[24] presents and explains different interoperability levels.

First level is Level 0, where isolated actors are not communicating at all. Level 1 establishes a basic communication, that requires a protocol compliant with the requirement of documented interfaces and data. Level 2 requires a common data format, complying with the requirement of a common reference model. A basic communication protocol is used on this level to structure the data. Level 3 introduces semantics of data, sharing the meaning of data over the systems’ actors. Level 4, pragmatic interoperability, requires that the systems’ actors are aware of other actors’ procedures and methods. This can either be reached by documentation or harmonization of the used procedures and methods. By doing so, the context of the shared information becomes visible. At Level 5, dynamic interoperability, systems are aware of the assumptions and constraints existing inside other systems. This means that a system must be aware of state changes which can occur in other systems during communication, hence respecting the effect on the results of the overall system. Level 6 defines the conceptual interoperability itself as an interoperability of system concepts. On this level, a system is fully specified and independent from its implementation. This sixth level emphasizes the provision and sharing of knowledge on the development, implementation and maintenance of the architecture. In the following sections the selected index to measure the technical interoperability are presented.

3.1.1 Technical Interoperability

A communication infrastructure is established allowing it to exchange bits and bytes, the underlying networks and protocols are unambiguously defined (Network connection standards such as HTTP; TCP/IP).

3.1.2 Syntactic Interoperability

A common protocol to structure the data is used; the format of the information exchange is unambiguously defined (WS-BaseNotification, CAP, URN syntax).

3.1.3 Semantic Interoperability

The meaning of the data is shared; the content of the information exchange requests are unambiguously defined (Dictionaries).

3.1.4 Pragmatic Interoperability

The use of the data – or the context of its application – is understood by the participating systems; the context in which the information is exchanged is unambiguously defined.

3.1.5 Dynamic Interoperability

The systems are able to comprehend the state changes that occur in the assumptions and constraints that each other is making over time, and are able to take advantage of those changes. In particular when interested in the effects of operations, this becomes increasingly important; the effect of the information exchange within the participating systems is unambiguously defined (e.g. interaction between thermal and PTZ cameras).

3.2 Managing & Procedural Interoperability Class

SECUR-ED with 40 partners has been a challenge also for the several entities to work together. This non-homogeneous team and the pragmatic experience on the demonstrator are the reasons why we decided to define the following three indexes, in order to consider also this aspect to measure the achieved interoperability level.

3.2.1 Interoperability as collaboration among several partners

SECUR-ED team included partners as Public Transport Operator (such as CRTM, RATP, ATM and DB), System Integrator (such as Thales, Ansaldo STS, Alstom or Bombardier), technologies provider (such as Nice, AXIS, Selex ES or Morpho), research centres (such as Technische Universitaet Dresden, INOV or Universitaet Paderborn).

3.2.2 Interoperability as collaboration among different organizations

In the same scenario, different organizations have collaborated, such as PTO, Fire Fighters, Police and Security Staff, each of them with different and strong regulations.

3.2.3 Interoperability as collaboration between public transport operators

In the same demo and scenario, different PTOs have collaborated, each of them with different internal organizations.

4 SECUR-ED Interoperability Results

4.1 Technological Interoperability

4.1.1 Interoperability of legacy systems within a SOA framework

The SECUR-ED demonstrations have highlighted the need for interoperability between legacy systems with new solution based on the SOA paradigm.

An example is the integration of an existing analog CCTV system in Milan into a people tracking solution and the SOCC requiring IP cameras and specific metadata support.

This has been reached by using a HW interface (an Encoder), in order to make available on the IP network the digital image of the analog video streams. On one side this solution permitted to integrate simply the legacy CCTV system into the new architecture and on the other side it opened the possibility for scalability of future-proof solutions.

Such digital solutions are prone to cyber-attacks. Therefore it is recommended, as for all ICT-based systems, to add also specific protections, like Firewalls or any other solutions to come, in order to guarantee service and data security.

4.1.2 Basic CCTV interoperability

International standards in video (ISO22311 and IEC62676) proved to be of great help regarding interoperability between different security and operational control centres.

Furthermore new CCTVs worked over IP with ONVIF CCTV protocol, with a smart interaction with other systems.

4.1.3 Video analytics interoperability

On technical side the SOA interface, consistently with IEC 62676, allowed a simple integration of video-analytics solutions with control centres, while basic CCTV standards allowed the integration with new and legacy CCTV systems. Some issues regarding installation and power supply have to be reviewed to improve the physical interoperability level, especially in rail environment.

4.2 Syntactic Interoperability

Public transport stakeholders have to deal with security threats and other rapidly changing crisis situations on a daily basis. To address this issue, different stakeholders have to be able to exchange and distribute relevant information in real time during daily operation. Working Group members (hereafter referred as WG), who represent both PROTECTRAIL and SECUR-ED, agreed to use an interoperability framework based on a Service Oriented (SOA) and Event Driven Architecture (EDA).

4.2.1 The interoperability framework

The WG have established an interoperability framework based on design patterns which were used in other industries successfully:

- follow the idea of an Service Oriented Architecture (SOA);
- using Event Based Architecture for data exchange between various security components and decouple the components with each other;
- re-use well established and proven standards, therefore reducing the non-recurring cost of software integration;
- plan an extendable architecture for the future to extend the framework with upcoming standards;
- build modular components with Web Services;
- support discoverable components to reduce the configuration effort and improve the reusability.

4.2.2 The Event Format

The WG developed a common **Event Format,** which includes as a minimum location, synchronized time, unique event identifier and type. Based on the evaluation study carried out by WG, Common Alerting Protocol (CAP) by OASIS for alerts was chosen as the best suitable reference standard for public transport sector. CAP is extensively used for weather warnings, Emergency Alert Systems, as well as new security related technologies such as Commercial Mobile Alert System.

The proposed minimum event format may be complemented by the following inherited CAP standard features:

- multi-operational and multilingual messages;
- three dimensional and flexible geographic description;
- message update and cancellation;
- security aspects like digital encryption and signatures;
- links to further information like images, reports and videos.

4.3 Semantic, pragmatic and dynamic interoperability

4.3.1 The information content of an event

Sharing information requires that the content of the information exchange requests are unambiguously defined.

The SECUR-ED event carries the following minimal standardised information that allows to reach a proper situational awareness at the different stakeholders levels:

- Unique Event ID;
- Event Start Time using Network Time Protocol (NTP : RFC 778, RFC891, RFC 956 and RFC 1305);

- Event Location in absolute coordinates (World Geodetic System year 1984 (WG84) or different references for underground infrastructures);
- Event Type.

4.3.2 Process interoperability

It's a strong business requirement that the complex event processing shall adapt automatically without programming. The business logic and workflow will be defined by business analysts and executed by integration platforms. This means that the business processes are modelled beforehand for operation and crisis procedures, guide the responders and operators through critical situations, enable a much faster response and an automatic information distribution based on the thread level. ISO/IEC standard 19510:2013, better known as Business Process Modelling and Notation (BPMN) is the right candidate to execute complex event processing in a graphical way.

4.4 Managing & Procedural Interoperability Results

Following the previous sections where Managing & Procedural interoperability indexes are explained, here the SECUR-ED results are collected:

- **Interoperability as collaboration among several partners:** Several European partners worked together to improve the security of Urban Public Transport services. The collaboration has been driven by the wish to reach the goal and by planned work, started from the definition of a common language until a pragmatic project management.
- **Interoperability as collaboration among different organizations**: The capacities were able to collaborate with different organizations thanks to configurable operative procedures.
- **Interoperability as collaboration between public transport operators:** The capacities were able to communicate with different PTO with different regulation. A procedural standardization was also applied, in order to have clear roles and procedure for the crisis management.

5 PTO Interoperability Feedback

In order to collect feedback from the Operator point of view, a questionnaire has been submitted to CRTM, RATP and ATM, operators involved respectively in Madrid, Paris and Milan demos. Interoperability analysis has not been applied to Berlin demonstration managed by DB, since it was focused on training, based on generic lessons developed in the project without involving technology interoperability.

The following table shows the capacity involved in the different demonstrators:

Demo / Capacity	Madrid	Milan	Paris	Berlin
Information management	x	x	x	
Telecommunications systems	x	x	x	
CCTV systems	x	x	x	
CBRNE systems		x	x	
Cyber security systems	x		x	
Training systems	x			x
Additional services	x	x		

The questionnaire included the following items:

- Does the specific test / activity involve different vendors / providers?
- Which is the level of standardization and legacy consideration?
- How the applied technologies or sub-system can really be considered as interoperable?
- How far the demonstrated technology or system is from the target of a wider interoperability of solution?

The different answers have demonstrated to what extent PTOs have concentrated their attention or have considered most important.

CRTM, the Madrid Demo Operator, has underlined the benefit of SOA to manage the solutions implementation, composed of several systems and modules, as SECUR-ED architecture and ICDs advised. The used Event data model, following SECUR-ED event schema, has ensured a good interoperability level among SECUR-ED capacities. Furthermore, high results have been achieved in term of integration of different stakeholders involved in the demo, (such as PTA, PTOs, LEFR, Emergency Services, etc.).

	Technological Interoperability [L=Low/M=Medium/H=High]	**Managing & Procedural Interoperability [L=Low/M=Medium/H=High]**
Supervision Server	M	H
Orchestration engine	M	H
Passenger Information	M	H
Operator work station	M	H
Fixed basic CCTV	M	H
Person tracking in video	M	H
Multi-Operator data exchange capacity	M	H

Table 5-1 Type A: Interoperability Matrix for Madrid Demo

RATP, the Paris Demo Operator, focused its feedback on technical and regulation issues: regarding experimented CCTV capacities, due to CNIL regulations, RATP had to install new cameras, but generally the solution can use all cameras already in place within the transport system. In general the level of interoperability is high, even if an extra effort has been identified as necessary to be fully interoperable: from the experimentation, geo-location and communication format required further investigations.

	Technological Interoperability [L=Low/M=Medium/H=High]	**Managing & Procedural Interoperability [L=Low/M=Medium/H=High]**
Supervision	H	H
CCTV basic services	H	H
Semi-automatic tracking	M	H
Massive fall detection	M	M
Facial recognition	M	H
Cyber protection	M	H
Toxic, Explosive and Radiological attack response	M	H

Table 5-2 Type A: Interoperability Matrix for Paris Demo

ATM, the Milan Demo Operator, have considered both technical and procedural aspects. Many actors have been included in the demo, not only SECUR-ED partners as capacity providers, but also different legacy providers and local Authorities. The experimentation returned good results, thanks to an effective procedural and managing method. Interesting experimentation has been done to test the interoperability level of SOCC of different stakeholders: no relevant technical issue has been raised with regards to the system of systems. The SECUR-ED architecture and ICD have been applied and worked, generally returning a high interoperability level.

	Technological Interoperability [L=Low/M=Medium/H=High]	**Managing & Procedural Interoperability [L=Low/M=Medium/H=High]**
Security Management System	H	H
Chemical and explosive Detection	H	L
Fixed Basic CCTV	M	L
Person Tracking in video	M	M
Radiological Detection - DIRAD	H	M
RFID ticket tracking	L	M
Communication Vehicle-Ground/Wayside	L	M
On-board Empty Vehicle Detection	M	H
Radiological Detection – Portal Monitor	M	L
Anti-Intrusion and Graffiti Prevention	L	M
Crowd Density Detection	M	M
Evacuation Modelling	H	M
Massive fall detection	M	M

Table 5-3 - Type A: Interoperability Matrix for Milan Demo

6 Way-forward

The observed good interoperability resulted from a project-wide implementation consensus, which does not apply naturally to individual stakeholders; this can only happen if approaches recognized as most promising are covered by international standards.

The following are the steps implemented within SECUR-ED (and in full cooperation with the PROTECTRAIL project):

- ISO22311:2012 “Societal security -- Video-surveillance -- Export interoperability” has been promulgated in November 2012 and SECUR-ED has demonstrated it during the Paris demonstration;
- Definition and promulgation of the IEC 62676 profile (with ONVIF CCTV and intrusion detection) matching the PTO’s CCTV needs while complying with legal requirements.

The notion of minimum standard Event Format and the issue of a standard localization within underground infrastructures could be introduced by the end of SECUR-ED in the European standardization roadmap (Mandate 487), but implementation remains to be done.

The main recommendations for the future are accordingly to monitor revisions of the above standards and contribute in the groups listed hereafter:

- IEC/TC9 (railway non-safety standards) adapting rail standards to integration of new security solutions with IEC 62580-2 On-board CCTV, which remains a hot and active topic;
- The eventing and associated geo-location standard activities to start within CEN TC391.

7 Conclusions

The objectives of SECUR-ED to validate integrated interchangeable, modular, scalable and interoperable security protection systems are successfully reached thanks to the smart choice to combine the SOA paradigm with the standard specifications realized by OASIS (Organization for the Advancement of Structured Information Standards), a global consortium that drives the development, convergence, adoption of e-business and web service standards.

According to this, SECUR-ED project has implemented the interface defined in PROTECTRAIL project to enable communications through services.

This proved to be not such a too big effort from the partners thanks to which it has been possible to achieve the project interoperability goal and to propose a set of standards applicable to security management for public transportation.

All demos highlighted how to use a general format to exchange all-hazard emergency alerts and public warnings, being the best way to disseminate information over all kinds of networks.

From a technological point of view, a strong effort has been done to make interoperable all solutions involved in the demo: this effort means costs, but once agreed, the protocol communication for transportation security information, having modular and almost “plug & play” technologies, shall be possible since technological and economic efforts shall be done just once. In fact it was also demonstrated, through satellite demonstrations, that this strategy is practically feasible, as a strong optimization of time and resources was effectively provided.

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 -