SECONOMICS

D1.3 - Airport Requirements final version

F. Quintavalli, A. Tedeschi, A. Pollini (DBL), B. Açikel, N. Ergün, U. Turhan (AU), M. De Gramatica, W. Shim (UNITN), Javier Cano, D. Rios Insua (URJC), J. Williams, M.Collinson (ABDN), S.H. Houmb, Thanh-Son Nguyen (SNOK)

Pending of approval from the Research Executive Agency - EC

Document Number	D1.3
Document Title	Airport Requirements final version
Version	2.1
Status	Draft
Work Package	WP 1
Deliverable Type	Report
Contractual Date of Delivery	31.01.2013
Actual Date of Delivery	13.12.2013
Responsible Unit	DBL
Contributors	AU, UNITN, URJC, ABDN, SNOK
Keyword List	Airport Security, Scenarios.
Dissemination level	PU

SEVENTH FRAMEWORK PROGRAMME

SECONOMICS Consortium

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

1	UNIVERSITÀ DEGLI STUDI DI TRENTO	Università Degli Studi di Trento (UNITN) 38100 Trento, Italy www.unitn.it	Project Manager: prof. Fabio MASSACCI Fabio.Massacci@unitn.it
2	DEEPBLUE	DEEP BLUE Srl (DBL) 00193 Roma, Italy www.dblue.it	Contact: Alessandra TEDESCHI Alessandra.tedeschi@dblue.it
3	Fraunhofer ISST	Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., Hansastr. 27c, 80686 Munich, Germany http://www.fraunhofer.de/	Contact: Prof. Jan Jürjens jan.juerjens@isst.fraunhofer.de
4	Universidad Rey Juan Carlos	UNIVERSIDAD REY JUAN CARLOS, Calle TulipanS/N, 28933, Mostoles (Madrid), Spain	Contact: Prof. David Rios Insua david.rios@urjc.es
5	1495 UNIVERSITY OF ABERDEEN	THE UNIVERSITY COURT OF THE UNIVERSITY OF ABERDEEN, a Scottish charity (No. SC013683) whose principal administrative office is at King's College Regent Walk, AB24 3FX, Aberdeen, United Kingdom http://www.abdn.ac.uk/	Contact: Prof. Julian Williams julian.williams@abdn.ac.uk
6	TMB Transports Metropolitans de Barcelona	FERROCARRIL METROPOLITA DE BARCELONA SA, Carrer 60 Zona Franca, 21-23, 08040, Barcelona, Spain http://www.tmb.cat/ca/home	Contact: Michael Pellot mpellot@tmb.cat
7	Atos	ATOS ORIGIN SOCIEDAD ANONIMA ESPANOLA, Calle Albarracin, 25, 28037, Madrid, Spain http://es.atos.net/es-es/	Contact: Silvia Castellvi Catala silvia.castellvi@atosresearch.eu
8	SECURENOK	SECURE-NOK AS, Professor Olav Hanssensvei, 7A, 4021, Stavanger , Norway Postadress: P.O. Box 8034, 4068, Stavanger, Norway http://www.securenok.com/	Contact: Siv Houmb sivhoumb@securenok.com
9	SOÚ Institute of Sociology AS CR	INSTITUTE OF SOCIOLOGY OF THE ACADEMY OF SCIENCES OF THE CZECH REPUBLIC PUBLIC RESEARCH INSTITUTION, Jilska 1, 11000, Praha 1, Czech Republic http://www.soc.cas.cz/	Contact: Dr Zdenka Mansfeldová zdenka.mansfeldova@soc.cas.cz
10	nationalgrid THE POWER OF ACTION	NATIONAL GRID ELECTRICITY TRANSMISSION PLC, The Strand, 1-3, WC2N 5EH, London, United Kingdom	Contact: Dr Ruprai Raminder Raminder.Ruprai@uk.ngrid.com
11	ANADOLU ÜNİVERSİTESİ	ANADOLU UNIVERSITY, SCHOOL OF CIVIL AVIATION Iki Eylul Kampusu, 26470, Eskisehir, Turkey	Contact: Nalan Ergun nergun@anadolu.edu.tr

Document change record

Version	Date	Status	Author (Unit)	Description
0.1	18/10/2012	Draft	A. Tedeschi, F. Quintavalli (DBL)	Proposed ToC
0.2	25/10/2012	Draft	U. Turhan, N. Ergun, B. Acikel (AU)	General airport Security Requirements and Regulations; Airport Operational Scenarios and Descriptions.
0.3	05/11/2012	Draft	U. Turhan, N. Ergun, B. Acikel (AU)	Selected and Refined Airport Operational Scenario.
0.4	17/12/2012	Draft	A. Tedeschi, F. Quintavalli (DBL)	First Draft for Scientific and Quality Check
0.4.1	19/12/2012	Draft	Matthew Collinson, Julian Williams (ABDN), Woohyun Shim (UNITN)	Scientific Review
0.4.2	21/12/2012	Draft	(UNITN)	Quality Check
0.5	07/01/2012	Draft	(DBL), M. De Gramatica, Woohyun Shim (UNITN), (ABDN), S.H. Houmb, Thanh-Son Nguyen (SNOK)	Modification proposed by scientific and υality Check. Alignement with D7.1 and D7.2.
0.6	09/01/2013	Draft	U. Turhan, N. Ergun, B. Acikel (AU)	Airport Security Structure and Stakeholders and Research Questions were defined for operational scenario.
0.7	15/01/2013	Draft	A. Tedeschi, A. Pollini (DBL)	Final Draft for Quality Check
0.8	18/01/2013	Draft	Javier Cano, David Rios Insua (URJC)	Scientific revision and contribution to Section 6. Modelling the Airport Case Study.
0.9	24/01/2013	Draft	Matthew Collinson, Julian Williams (ABDN), E. Chiarani, Woohyun Shim (UNITN)	Scientific Review and Quality Check
1.0	28/01/2013	Draft	A. Pollini, A.Tedeschi (DBL)	Final Version
1.1	30/11/2013	Draft	A. Pollini, A.Tedeschi (DBL)	Revision to the Final Version according to Mid-Term Review reccomendations
1.2	10/12/2013	Draft	Julian Williams (ABDN), Woohyun Shim, Fabio Massacci (UNITN)	Review and comments
2.0	12/12/2013	Final	A. Pollini, A.Tedeschi (DBL)	Final revision
2.1	13/12/2013	Final	E. Chiarani (UNITN)	Final version for submission

INDEX

Executive summary

This deliverable presents the final version of Airport Security requirements with respect to Work Package 1 of the SECONOMICS project. It follows on from the work documented in SECONOMICS Deliverable 1.2 titled 'Airport Requirements – First Version'.
D1.3 focuses on analysing the following point: summarizing the main regulatory frameworks that apply to airport security operators; presenting current and emerging vulnerabilities and threats in the airport domain; select the most relevant ones for the SECONOMICS modelling workpackages and structure them into 3 Airport Security Scenarios.

The high level Airport Security Policy Scenarios (1 and 2) and the low level Airport Operational Security Scenario (3) have been constructed to cover the detail airport security requirements and open issues already identified in D1.2:

(1) the Security Measures Scenario,
(2) the Training of Airport Personnel scenario,
(3) the Unlawful Access to Tower Scenario.

The presented scenarios examine the current situation from social and economic costs: costs of technology and costs of human resources are just two examples of that. This can be adapted to airport of different sizes, starting from the low costs ones to the spoke and hubs.
The proposed scenarios will be used as a first basis to steer the model development and to serve as proof of concept for model assessment and validation. During the project lifecycle they may be adapted and modified according to stakeholders' needs and scientific WPs research interests.

In order to accomplish these objectives D1.3 has been organized as follows. It firstly sets up the context describing Aviation Security Regulations, the main Policy Makers at Worldwide, European and National Level and the airport security stakeholders.
Then the deliverable describes in details the scenario selection process, the stakeholders engagement and all the activities carried out by WP1 partners to gather relevant data and domain information from airport security stakeholders.
Finally, the three scenarios identified are described in details, referring to the relevant operational and regulatory issues. For each scenario the relevant research questions are stated and the modelling techniques adopted by Scientific WPs to address them are briefly described.

Three annexes complement D1.3. The first Annex (Section 7) discusses economic issues focusing on airport expenditures and revenue mechanisms. The second Annex (Section 8) integrates the regulatory framework by describing those additional security measures applicable in exceptional cases. The last Annex (Section 9) provides additional knowledge for the training scenario detailing the International Air Transport Association (IATA) security training portfolio.

DBL and AU contributed to the production of this deliverable as airport domain experts by providing the airport security background knowledge. UNITN and ABDN provided inputs about the WP6 research questions and modelling approaches. URJC contributed to

the inclusion of WP5 modeling strategy for the airport case study. The scientific partners reviewed the proposed scenarios in order to assure the applicability of their models to the selected cases. SNOK reviewed the document in order to integrate the Airport Security requirements into WP7 initial framework.

1 Introduction

1.1 Scope of the report

This report will identify and analyse the main issues for airport security by listing the stakeholders, their mutual interactions and their requirements with reference to key scenarios that have been selected in WP1. A range of techniques will be used, from interviews of key stakeholders, ethnographic observation, and the collection of quantitative indicators whenever possible. Some of the key issues that will be addressed in this deliverable are:

- describe the scenarios for both high level and operational aspects of airport structure,
- provide insights about economic and sociological issues of airport security,
- address the research questions proposed by the technical workpackages,
- introduce the modelling of the case study.

The outcome is a report describing operational, economic and sociological issues in airport security. The report describes the situation from the passenger point of view as well as from an organisational and policy-makers point of view. The societal impact and passengers and operators acceptance of security-driven decisions will be taken into account in all the proposed scenarios.

1.2 Project Objectives and Expected Results

The main objective of SECONOMICS is to develop innovative security modelling and analysis techniques and tools that will support policy makers in security-related decisions by taking into account also social and economic factors. This is particularly challenging when considering both logical and physical security aspects and different domains in a pan-European perspective. The practical relevance of SECONOMICS research will be validated against three challenging domains, i.e. Airport, Critical Infrastructures and Urban and Local Transport that offer most research challenges and greatest long-term business opportunities. Following this, the final goal is to understand the needs of security in the different domains: models, software tools and guidelines for Policy Makers are the outputs. Especially first and last points are the core of the project, considering them as a real help for people and/or organisations that are responsible for taking decisions. This means that the contribution of the project is to develop and improve the way that Policy Makers face security issues, which interact with technical and socio-economic problems within a complex context.

1.3 D1.3 contribution to project objectives

The high level objective of WP1 is to provide scope for the various cases of interest to SECONOMICS in repsect of air transport.
The specific objective are:

- Objective 1. Identifying and analysing the current main security concerns of the airport world, in order to feed the economic modelling WPs.
- Objective 2. Validating the risk model and the economics models, both in ensuring the achievement of appropriate models and towards their final validation wrt to their efficacy and usability in the Airport domain.

- Objective 3. Validating the decision-making tool, by means of live trials whenever feasible.

In particular D1.3 (together with D1.2) aims to accomplish Objective 1. In order to reach this goal, the Airport Case Study activity was concerned both with the identification of the operational needs of Airport Stakeholders and the establishment of appropriate Scenarios to steer and evaluate SECONOMICS technical solutions. Objective 2 will be addressed by D1.4 Model Validation, while all the activities carried out to achieve Objective 3 will be reported in D1.5 Tool Validation.

The development of Deliverable D1.3 has followed an iterative and participative process to ensure that the needs are properly expressed. Scenarios are well understood and adapted to the project scope and adequate domain knowledge has been gathered by airport security stakeholders. As first and preparatory step an Expert Group of Airport Stakeholders has been created and involved in Scenarios definition and Airport Security Requirements collection. The Expert Group is composed by representatives of:

- Airport Management Organisations,
- Air Navigation Service Providers (ANSP),
- Security Managers,
- the Aviation Authority,
- Airspace Users and Technology Providers.

1.4 Overview of the document

Deliverable 1.2 sets the scene in the airport security area which is covered in more detail in this document, the final version of the ‘Airport Requirements’. The remainder of this report is structured as follows:

- **Section 2** Introduction and background to Airport security domain

  This section describes the evolution of threats and attacks in aviation and airport security and how the European Aviation security framework development ran in parallel. The Airport Regulatory Authorities and the Airport stakeholders security costs, financing and revenues are also described.

- **Section 3** Stakeholders & Engagement Plan

  This section lists all the stakeholders involved in WP1 as well as the activities through which they have been involved.

- **Section 4** Scenario definition

  This section describes the selection process for both high level Security Policy and low level Airport Security scenarios and the research questions that guide scenarios’ implementation.

- **Section 5** Modeling the Airport Security case studies

  This section briefly introduces the WP5 and WP6 modelling approaches and ensures that they are applicable in airport security domain. To have a more detailed theoretical introduction to the modelling techniques applied to WP1 scenarios please refer to D5.1, D5.2 and D6.1 deliverables.

2. Further background to Airport Security

This section provides an historical background of Airport Security by describing how threats and attacks have evolved and differentiated in the last decades. The section also describes the aviation security regulatory framework, i.e. authorities and regulations.

2.1 Evolution of threats and attacks in aviation and airport security

Security has always been a priority for the European aviation industry. Terrorist attacks have been catalysts for change in how aviation security measures have developed and improved its standards and their implementation across Europe over the years.

Since its early beginnings, the aviation industry has been a target for acts of violence and terrorism and the most major advances in aviation security have occurred as a consequence of terrorist activities. Three distinct phases can be distinguished during the last 65 years [1]. They are detailed in the following.

Phase 1: 1948 to 1968 – Escape from persecution

Spanning 1948 to early 1968, this era was characterised by air piracy or 'hijacking' of aircraft where individuals fleeing a State to avoid persecution or prosecution viewed hijacking aircraft as a fast and convenient means of achieving this aim. Hijacking has reduced from that period, even though recent events in China demonstrate that it is not totally obsolete. During the early part of 2003, a number of hijackings were reported where individuals were attempting to reach Taiwan from China.

Phase 2: 1968 to 1994 – The political phase

If aviation terrorism Phase 1 was mainly apolitical, 1968 is seen as the beginning of 'modern terrorism' and the link between politics and terrorism against civil aviation.

Although hijacking was still the civil aviation terrorist's most popular tactic (between 1967 and 1996, of the 1,033 incidents against airlines 914 (88%) were hijackings), the terrorist organisations began to use hijackings and bombings as a way of calling attention to their cause. This means that specific objectives of these attacks were invariably to:

- Embarrass their opponents (governments and other terrorist organisations).
- Damage the economy of the target State.
- Use it as a tool for extortion, either for the release of imprisoned colleagues and/or for money.
- Engender terror (fear) in the population

This phase is marked by three significant acts of aviation terrorism, as a consequence of some of them security regulations have been defined.

- In June 1985, Lebanese terrorists diverted TWA flight 847 en route from Athens to Beirut.
- One passenger was killed during the two-week ordeal; the remaining 155 passengers were released. This hijacking, together with an upsurge in Middle East terrorism, resulted in a number of US actions, among them the International Security and Development Cooperation Act [2].
- 1985 also saw the bombing of an Air India flight when ground staff allowed a bag with no confirmed seat holder to be checked through to its final destination. This

incident led to the inauguration of the International Civil Aviation Organisation's (ICAO) Aviation Security Panel and the rewrite of Annex 17 [3] (Annex 17 of the Convention on International Civil Aviation is a Security manual containing operating guidelines and Training Programmes – it is considered the 'rulebook' on aviation security and outlined later in this section).

- On 21 December 1988, enroute from London to New York, a bomb brought down Pan Am flight 103 over Lockerbie, Scotland. All 259 people onboard were killed, as well as 11 people on the ground.

Phase 3: 1994 to date – The aircraft as a weapon of destruction

The Algerian terrorists hijacked Air France flight 8969 in December 1994, started the current phase of aviation and airport security terrorism. During the flight from Algeri to Paris the French government refused the aircraft landing rights at Paris as they had received intelligence that the hijackers intended to blow up the aircraft over the city. On diverting to Marseilles, French police commandos stormed the aircraft and successfully rescued the passengers and crew. This incident marked a change in tactics for terrorists: international civil aviation had become a battle ground for terrorists and aircraft a weapon.

The 11 September 2001 attack to the New York World Trade Centre has been the most striking case of aircraft used as a weapon. The events of 11 September 2001 signalled a major change in terrorist activity. With the advent of suicide attacks, the intention is to inflict maximum collateral damage and loss of life.

This unprecedented attack resulted in an immediate and drastic heightening of air transportation security across the world.

2.2 European Aviation Security Framework

As previosuly noted, improvements to aviation security have been historically reactive, responding to crisis as it occurs. States have adopted (or not) recommendations put forward by the various international bodies resulting in an approach that is disjointed and incremental rather than a coherent global standardised system essential to address the growing terrorist threat.

Based on European Civil Aviation Conference (ECAC) Document 30 [4], the European Commission proposed the adoption and enforcement of common security rules for civil aviation across the Member States aiming to increase aviation security at national and international level.

The main objectives of the new regulations were to:

- Establish and implement appropriate Community measures, in order to prevent acts of unlawful interference against civil aviation.
- Provide a basis for a common interpretation of the related provisions of the Chicago Convention, in particular its Annex 17 [3].

These objectives were achieved by the setting up of common basic standards for aviation security measures and appropriate compliance monitoring mechanisms.

The rules were predominantly concerned with:

- Control of access to sensitive areas of airports and aircraft.
- Control of passengers and their hand luggage.
- Control and monitoring of aircraft hold luggage.
- Control of cargo and mail.

- Training of ground staff.
- Definition of specifications for the equipment for the above controls.
- Classification of weapons and other prohibited items

The level and quality of aviation security in Europe is widely considered to have improved significantly since the introduction of Regulation (EC) No 2320 / 2002 [5] together with a system of legally-binding inspections. The Commission inspections programme is ensuring that the legislative standards are mandated on the Member States and do apply not only in theory but in practice in the European Union.

2.3 Description of Aviation Authorities

2.3.1 International Civil Aviation Organization (ICAO)

ICAO is the International Civil Aviation Organization and "works to achieve its vision of safe, secure and sustainable development of civil aviation through the cooperation of its Member States" (*http://www.icao.int/Pages/vision-and-mission.aspx*). When ICAO has been created, in 1944, no one foresaw the need to specify anything regarding the Security topic, either for airplane or aerodromes. In the late 1960s, Security arose as serious issue, and during the 1974 Chicago Convention, Annex 17 [3] was first disseminated (there are several Annexes for different topics), and on 1st July 2011 the 12th amendment has become applicable. With the advent of Annex 17 [3], ICAO began providing States with guidance material to assist with the implementation of international security measures. ICAO's activities continue in terms of security audits to the several associations involved in the program and to the State Members which are not able to address serious security deficiencies: travel documents (for passengers, crew, luggage, cargo and mail) and training to security personnel (development of course material and conduction of workshops and seminars) are the key points.
ICAO gives minimum standards which every State Member must satisfy in order to be part of it (and to have the possibility to have flights on its own territory). This means that every State Member has to build a *civil aviation structure*, which has to satisfy the minimum standards, and share it with the rest of the world.

2.3.2 European Civil Aviation Conference (ECAC)

The European Civil Aviation Conference (ECAC) is the organisation of 44 European Member States forming an integral part of the ICAO global air transport family and deals with all aspects of civil aviation. ECAC's aims to promote the continued development of a safe, secure, efficient and sustainable European air transport system. ECAC seeks to harmonise civil aviation policies and practices amongst its Member States, and to promote discussions on policy matters between its Member States and other regions of the world. ECAC satisfies ICAO minimum standards, and in many ways goes beyond them, in order to increase the safety and security on aircraft and inside aerodromes.

A similar organisation is the FAA (Federal Aviation Administration) in US. Regarding the Security Topic, ECAC issued several different laws, which have been modified and amended, and nowadays the most important are the REGULATION (EC) No 300/2008 [6] and the COMMISSION REGULATION (EU) No 185/2010 [7]. The first one repeals the Regulation (EC) No 2320/2002 [3] and concerns common rules in the field of civil

aviation security, not going in deep details, as the latter does, regarding the implementation of rules.
For example, in the EC No 300/2008 [6] it is stated that, within European Union, the one-stop security (screening for passengers and luggage only at the starting point of the journey) has to be performed (*rule No 20*); rule *No 13*, instead, states that every Member State should draw up a national civil aviation security programme (NSP).

2.3.3 Civil Aviation Authorities (CAA)

A **civil aviation authority** (**CAA**) is a government statutory authority in each country that oversees the approval and regulation of civil aviation. The CAA is responsible for the definition of the National Security Program (NSP). In the NSP there are the general rules for each airport operator, airline, etc. which should be followed, in terms of airport and on-board security, passengers, luggage, mail and goods screening, airport and on-board supply, recruitment and training for personnel. Each State Member has to implement the NSP in order to check the level and quality of civil aviation security within its own territory, at the same time complying the ECAC Regulation and Recommendations.

One of the first chapters of the NPS regards the commitment for every air carrier and airport operator, including handlers and service provider, to have a security programme, which has to comply the above mentioned European rules and has to be approved by the national Civil Aviation Authority of the Member State in which the subject is operating. Moreover, the programme shall include internal quality control provisions describing how compliance with these methods and procedures is to be monitored by the operating subject.

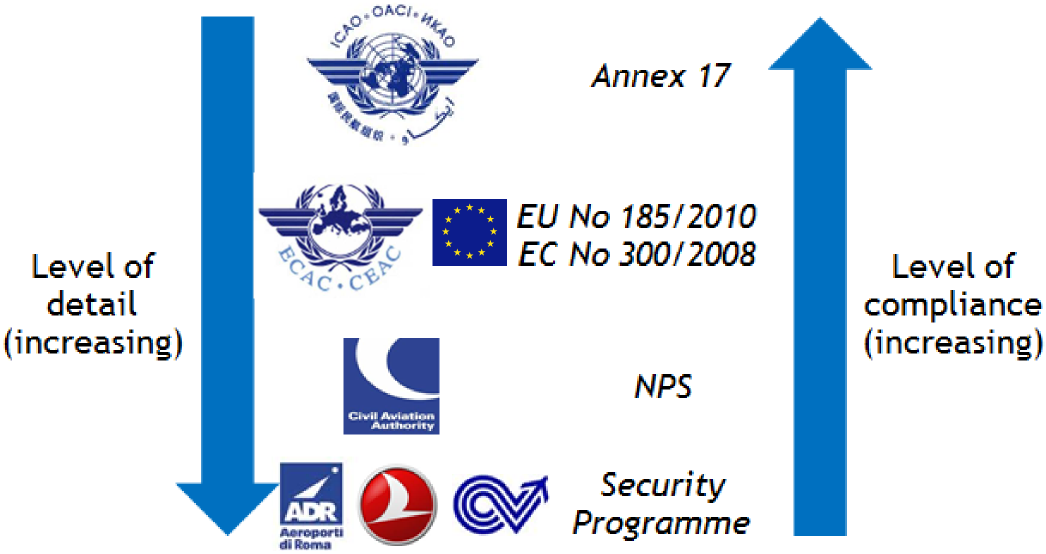
Level of detail (increasing)
Annex 17
EU No 185/2010
EC No 300/2008
NPS
Security Programme
Level of compliance (increasing)

Figure 1 - Worldwide, European and National Regulations.

Figure 1 describes the level of detail, which increases from the ICAO to the airport stakeholders, considering the number of information given in each "document" and who they are addressed to. The right arrow, instead, explains that the lower level (in terms of detail) has to comply with what is stated in the above one. The next paragraph gives an overview of rules, laws and regulations.

2.4 Regulations

2.4.1 ICAO General Requirements About Airport Security

ICAO [7] is identifying the security objectives for member states as below:

- Each Contracting State shall have as its primary objective the safety of passengers, crew, ground personnel and the general public in all matters related to safeguarding against acts of unlawful interference with civil aviation.
- Each Contracting State shall establish an organization and develop and implement regulations, practices and procedures to safeguard civil aviation against acts of unlawful interference taking into account the safety, regularity and efficiency of flights.
- Each Contracting State shall ensure that such an organization and such regulations, practices and procedures:
    a) Protect the safety of passengers, crew, ground personnel and the general public in all matters related to safeguarding against acts of unlawful interference with civil aviation; and
    b) Are capable of responding rapidly to meet any increased security threat.
- Each Contracting State shall ensure that the appropriate authority arranges for the supporting resources and facilities required by the aviation security services to be available at each airport serving civil aviation.
- Each Contracting State shall ensure that persons other than passengers, together with items carried, being granted access to security restricted areas are screened; however, if the principle of 100 per cent screening cannot be accomplished, other security controls, including but not limited to proportional screening, randomness and unpredictability, shall be applied in accordance with a risk assessment carried out by the relevant national authorities.

ICAO Doc Volume III is about Airport Security Organization, Programme and Design Requirements. Especially airport airside development requirements are:

- The border between the landside and the airside is called the perimeter of the airport. The perimeter of a security restricted area may be defined by a natural boundary, by free-standing fences or walls, by the outer walls of a building or by divisions within it. Its function is to provide a degree of physical, psychological or legal deterrence to intrusion. Its effectiveness as a security measure may be enhanced by the deployment of perimeter intrusion detection systems (PIDS), a closed-circuit television (CCTV) system, security lighting and patrols by guard forces. (See Appendix 2 for information on perimeter protection.) All underground access (rivers, culverts for drainage or cables wider than 80 cm) should be closed and/or made accessible to an appropriate standard.
- Airside development should (where appropriate) provide for the following:
  a) Physical security measures for the airport perimeter and security restricted areas;
  b) Perimeter roadways and other access roads for patrol purposes;
  c) Security and apron lighting;

d) Vehicle and pedestrian access points to the perimeter and security restricted area, including automatic access control systems;
e) Electronic intrusion detection systems;
f) An isolated aircraft parking position for the searching of aircraft subject to specific threats or acts of unlawful seizure;
g) A blast containment area for suspect explosive devices;
h) explosive-detection equipment for cargo containers and pallets;
i) Facilities for kennelling and training explosive-detection and patrol dogs;
j) A simulation chamber.

2.4.2 ECAC General Requirements about Aviation and Airport Security

Aviation security objectives and responsibilities of member states are given in the ECAC Doc 30 [4] Part II as:

- In order to protect persons and goods within the ECAC region, acts of unlawful interference with civil aircraft that jeopardise the security of civil aviation should be prevented by establishing common rules for safeguarding civil aviation.
  The means of achieving the above-mentioned objectives should be:
  a) The setting of common basic standards on aviation security measures;
  b) The setting up of appropriate compliance monitoring mechanisms. [1] art 1.2.
- Member States should ensure the application in their territory of the common basic standards referred to in 1.1. Where a Member State has reason to believe that the level of aviation security has been compromised through a security breach, it should ensure that appropriate and prompt action is taken to rectify that breach and ensure the continuing security of civil aviation. [1] art 4.5.
- Member States may derogate from the common basic standards referred to in 1.1 and adopt alternative security measures that provide an adequate level of protection on the basis of a local risk assessment at airports or demarcated areas of airports where traffic is limited to one or more of the following categories:
  1. Aircraft with a maximum take-off weight of less than 15000 kilograms;
  2. Helicopters;
  3. Law enforcement flights;
  4. Fire suppression flights;
  5. Flights for medical services, emergency or rescue services;
  6. Research and development flights;
  7. Flights for aerial work;
  8. Humanitarian aid flights;
  9. Flights operated by air carriers, aircraft manufacturers or maintenance companies, transporting neither passengers and baggage, nor cargo and mail;
  10. Flights with aircraft with a maximum take-off weight of less than 45500 kilograms for the carriage of own staff and non-fare paying passengers or goods as an aid to the conduct of company business, in [3], art1.

ECAC made identifications about aviation security in its Document [4], as below:

- The primary objectives of aviation security are to ensure that the travelling public, crew, ground personnel and the general public are protected from acts of unlawful interference and that public confidence in aviation security is retained;

- The threats to civil aviation and the risk of acts of unlawful interference are likely to persist in the foreseeable future and will present themselves in many different forms of attempted violence;
- The security measures should be proportionate to the perceived threat and duly adjusted to the special circumstances of each type of civil aviation activity;
- These measures should be kept under constant review and may have to be supplemented by additional measures adapted to increased and/or new threat situations;
- All Member States are expected to apply the provisions of Annex 17 [3], the provisions in other ICAO Annexes and PANS documents which are reproduced in the green pages of [7], the relevant ICAO Assembly Resolutions and the guidance material in [8];
- all Member States should implement harmonised basic security measures with the objective of achieving an acceptable and uniform level of security at all airports and by all air carriers in the ECAC region and maintaining consistency with European Union regulations; and
- All Member States, when determining the scope of measures and methods for ensuring aviation security, should be guided by the security objectives, common principles, procedures, technical specifications, criteria, guidance material and/or information contained in the following recommendations representing a consolidated statement of the continuing ECAC policies and associated practices in the field of aviation security;

2.4.3 ECAC Identifications for Air Traffic Management Security

ECAC Doc 30 [4] includes Air Traffic Management security in its chapter 13 as following:

Objective: Each Member State should protect the air traffic management (ATM) system and air navigation services, including from acts of unlawful interference that could disrupt the continued provision of air navigation services, through policy and procedures that take into account the requirements for the safety, regularity and efficiency of flights.

Application: This protection should apply to the Air Navigation Services (ANS), Air Traffic Management (ATM) and Communication, Navigation and Surveillance (CNS) assets and personnel.

Responsibility: Each Member State should designate a relevant authority within its administration to be responsible for the oversight and coordination of ATM Security.

General principles: Each Member State should ensure that Air Navigation Service Providers within its jurisdiction establish a Security Management System; to ensure the protection of critical Air Navigation Services, ATM and CNS assets and personnel from unlawful interference that could significantly threaten or disrupt the continued provision of air navigation services. This should include measures in the following areas:

- Personnel security,
- Physical security,

- Operational Information and Communication Technology (ICT) security, including protection of IT infrastructure to ensure the collaborative support and contribution to aviation security, national security and defence.

Each Member State should ensure that the Appropriate Authorities, other national authorities concerned with the security of airports, ANSPs or CNS/ATM assets work closely together to ensure a complementary and layered approach based on a mutually agreed level of criticality and security risk.

2.5 Airport Stakeholders Security Costs, Financing and Revenues

Security related responsibility

- Airport security: the airport is generally responsible for airport security, with the exception of background checks on staff IDs and external public areas. Some of the activities can be carried out by a combination of private firms and police services.
- Terminal surveillance, airside and perimeter patrols - these are predominantly the responsibility of the police services and private security companies.
- Aircraft security – protection of aircraft is primarily the responsibility of the carrier. This includes searching and checking of the aircraft.
- Passenger and baggage screening - this is carried out by a combination of airport, police services and private security companies. The performance of these activities is almost equally shared between these parties across the States.
- Baggage reconciliation and protection - this is generally the responsibility of the carriers.
- Cargo, courier and express mail – the screening of cargo, courier and express mail is generally the responsibility of the carrier.
- General aviation - Checks on general aviation users are usually conducted by the airport operator or private security companies. In few States, the police are responsible for this activity.

Models for the provision of European aviation security

There are two basic models for the provision of aviation related security activities within Europe:

- Centralised Model – the main security activities are primarily the responsibility of the State via a government body (CAA, Ministry of Transport, police force, etc). This is broadly the situation in 11 States (Austria, Finland, Germany, Iceland, Italy, Luxembourg, Norway, Portugal, Spain, Sweden and Switzerland).
- Decentralised model – the main security activities are provided by the airport authorities under the supervision of the relevant authority (normally the CAA).
These activities could either be provided by the airport directly or outsourced to a third party. This is broadly the current situation in 7 States (Belgium, Denmark, France, Greece, Ireland, Netherlands and the UK).

This diference is mainly due to political, social and historical reasons and not strictly to quantitative economic evaluations.

As reported in [1], some changes in how security activities are provided have been seen in the Netherlands. The airports have taken over responsibility for the main activities from 1st April 2003 from the Dutch Border Police. In Norway with the enacting of the Regulation in May 2004, a more decentralised approach is being followed. Greece is also considering transferring responsibility for the provision of the main security activities to the airports.

3 Stakeholders & Engagement Plan

This section lists the airport security stakeholders involved in the WP1 Expert Group. It also describes the 1st year in which they have been involved and the future engagement plan for 2nd year of the project.

During the course of the SECONOMICS project the Airport Security case study responsibles will engage with a number of stakeholders and stakeholder groups. These stakeholders are put into the Expert Group of Airport Stakeholders, composed of:

- representatives of Airport Management Organisations,
- Air Navigation Service Providers (ANSP),
- Security Managers,
- the Aviation Authority,
- Airspace Users and Technology Providers,

For each stakeholder (or stakeholders' group) the table below lists the representatives at European Level which have been iteratively involved in WP1 data gathering activites.

Airports	ANSP	Airlines	Civil Aviation Authorities	Training Providers	Technical Providers
Falconara/Aerdorica(Italy) Abruzzo-Pescara/ SAGA (Italy) Fiumicino/ADR (Italy) Esbjerg Airport (Denmark) Tbilisi Airport/TAV (Georgia) Brno/ LETIŠTĚ (CZ)	ENAV (Italy)	Alitalia (Italy) Meridiana (Italy)	AESA (Spain) ENAC (Italy)	ENAC Certified Instructors (Italy) IATA Certified Instructors (All Europe)	Thales Italia - Security Service&Solutions (Italy)

Table 1. Stakeholders' Representatives

During the SECONOMICS first year we carried two main iterations with Airport Stakeholders:

- the first one to define, evaluate and review relevant Security Scenarios, and
- the second one to start collecting inputs for the modeling activity to be carried out during the second year of the project.

A range of data gathering techniques have been used to carry out the stakeholders needs identification activities, from interviews of key stakeholders, focus groups, written questionnaires and ethnographic observation, collection of quantitative indicators. Table 2 shows the year 1 stakeholders' needs identification activities.

Year 1		
Stakeholders Needs Identification		
Timeline	Activities	Involved Actors
M1-M3	Stakeholders Identification and Preliminary Contacts Literature and document Review, Interviews	ANSP (ENAV), Airlines (Alitalia, Meridiana), Airport Management Organisations (ADR, Aerdorica, Pescara Airport), ICT Airport Security Solution Industry (Thales)
M4	Introduction to Airport Security Issues Airport Operational Security Needs Definition Focus Group	Spanish and Italian Civil Aviation Authorities, IATA Security Instructors, Ancona-Falconara Airport and Pescara Airport
M3-M6	Scenario Definition	Project Consortium Members and Airport Security Stakeholders
M5-M6	Scenario Validation and Refinement Interviews	ANSP (ENAV), Airlines (Alitalia, Meridiana) and Airport Management Organisations (ADR, Aerdorica, Pescara Airport)
M5-M6	High-level Requirements Definition	Consortium Partners (End Users and Domain Experts)
M6-M12	Scenario and High-level Requirements Review Overview of the Airport Regulatory Framework, focus on Security Training	Airport Stakeholders, Certified Security Instructor, Certified Security Instructors, Interviews with Airport Security Managers, End User Consortium Partner
M10-M12	Collection of Quantitative inputs to inform the analyses and modeling activities of technical WPs.	Airport Management Organisations (Aerdorica) and End User Consortium Partner

Table 2. 1st Year Stakeholders' needs identification process

3.1 Future Stakeholder Activities

The implementation of Task 1.2 Model Validation activities foresee further stakeholder activities for M10-M21. In particular three phases are planned to be held:

Phase 1 – Data collection (M12-M16)

- Expert Judgement involving Aviation and IT Security Experts
- Interviews with Airport Security Managers (Anadolu, Falconara, Esjberg, Pescara Airports)

Phase 2 - Models finalization (M17-M19)

- Expert Judgement involving Aviation and IT Security Experts
- Document analysis: Analysis of Aviation Security Official Regulations and Security Reports
- Passengers Survey Research in Anadolu Airport about Security Perception

Phase 3 – Validation (M20-M24)

- Evaluation Criteria Definition with Aviation and IT Security Experts
- Airport Security Workshops
  - In-itinere validation at Falconara Airport – Management Board
  - Final validation at Anadolu Airport - Management Board and School of Aviation scientific committee.

  Activities: Elicit decision making processes as baseline for Models evaluation
  Models Walktrough
  Experiment with Models on selected Scenarios

- Models and Modelling Refinement involving Technical Partners, Domain Experts and End-Users
- Final Evaluation of Modelling Approaches and Models in dedicated Workshops (in Rome and in Anadolu) jointly with exploitation&dissemination activities

Last year of the project will see WP1 stakeholders mainly involved in validating the decision-making tool, by means of live trials at different stages of development of the tool.

4 Airport Security Scenarios

This section outlines the iterative scenarios' definition process and describes the rationale behind the selection of each scenario. The scenarios are also detailed with the security operational and policy-making aspects needed for the analysis and modelling activities carried out in WP4, WP5 and WP6.

Relevant research questions have been identified and discussed for each selected scenario.

The WP1 scenario development process described in this section led to the selection of the following three scenarios:

(1) the Security Measures Scenario,
(2) the Training of Airport Personnel scenario,
(3) the Unlawful Access to Tower Scenario

A variety of relevant threats have been analysed in literature and discussed with domain experts, ranging from drug and human trafficking to smuggling, until cyber and bio-terrorism and other criminal activities.

WP1 decided to focus on the airport security decision-making and policy making (i.e. Implementation of Security Measures), which offered the opportunity to analyse the bidirectional influence of events occurring at operational level and the decisions at policy level on budget and resource allocation.

The second scenario investigates how organisational and human aspects affect airport security (i.e. Training of Airport Personnel). It was considered very relevant by many stakeholders since lack of Security Culture has been identified as a main vulnerability for most organisations.

The last scenario, on the physical attack to airport infrastructure (i.e. Attack to Tower), resulted to be one of the most widespread threat to airport security that impacts on security investment and certainly provokes social impact (e.g. due to resonance on media).

According to expert judgement, among the security threats that have been analysed, Cyberthreats ought to be mentioned as one of the most promising insightful scenario to discuss with the WP1 stakeholders and develop as future result within WP1 airport security scenario definition.

4.1 Scenarios Selection Process Update

The Scenario selection process has been implemented in a first phase (M3-M6) (see Table 2 as reference), during which WP1 stakeholders have been involved in the early formulation of scenarios review and evaluation activity, and a second phase (M7-M12), during which the revised version of the scenarios have been validated and ultimately selected. Figure 2 summarizes the two phases.

Review and evaluation of early formulation of scenarios
Validation of final and revised version of scenarios

Figure. 2. Scenario Selection Process

In order to select proper scenarios to steer the modelling and development of SECONOMICS framework and tools, it has been decided to focus on both:

- low level Airport Security scenarios that describe how local decisions are affected by the implementation of single security measures in specific cases.
- high level Security Policy scenarios that represent general aspects of airport security currently under discussion worldwide by institutional stakeholders

Experts of airport domain are Deep Blue and Anadolu University. AU and DBL are responsible to create scenarios at two different levels of abstraction, which are addressed by two different stakeholders:

- the low-level Airport Security scenarios will interest decision makers of the airport, so it is possible to be defined as local;
- the Security Policy scenarios, instead, will be interest of Regulator and Policy Makers (National Civil Aviation Authorities and other organisation).

The picture below shows the scenarios’ development process and introduces the scenarios themselves.

DBL have initially worked on Passenger-Baggage Reconciliation, Body Scanner introduction and Training of Airport Personnel; whilst AU have initially focused on Unlawful Access to the Tower, Unlawful Interference with Apron, Unlawful Interference with Airside and Unlawful Interference with Security Checks.

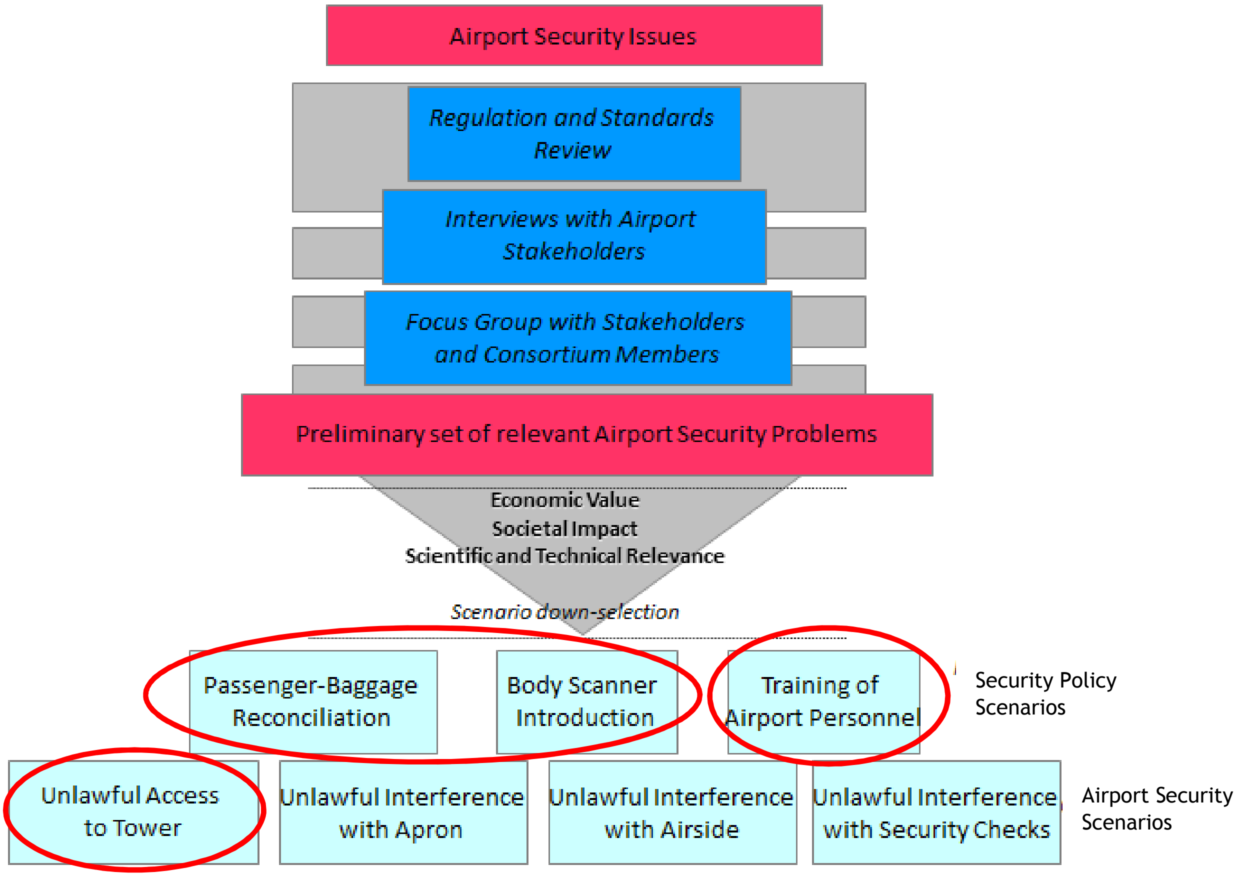
Airport Security Issues
Regulation and Standards Review
Interviews with Airport Stakeholders
Focus Group with Stakeholders and Consortium Members
Preliminary set of relevant Airport Security Problems
Economic Value
Societal Impact
Scientific and Technical Relevance
Scenario down-selection
Passenger-Baggage Reconciliation
Body Scanner Introduction
Training of Airport Personnel
Security Policy Scenarios
Unlawful Access to Tower
Unlawful Interference with Apron
Unlawful Interference with Airside
Unlawful Interference with Security Checks
Airport Security Scenarios

Figure. 3 Process of Scenarios Development and Selection

Following the research questions provided by Technical Workpackages, three Scenarios were finally selected, two Security Policy scenarios and one Airport Security scenario.

The two Security Policy Scenarios were:

(1) the *Security Measures* Scenario, that merges and integrates
- the *Passenger – Baggage Reconciliation* Scenario, and
- the *Body Scanner Introduction* Scenario;

(2) the *Training of Airport Personnel* scenario.

The Airport Security Scenario proposed was:

(3) the *Unlawful Access to Tower* Scenario.

They will be detailed in next Section.

4.2 Security Policy Scenarios

The two selected Scenarios are described in details with respect to current European Regulations and their suggested implementation in Airports. Further details about Security Measures and examples of Training Courses delivered by European and Local Institutions are provided in the Annexes.

4.2.1 Security measures (Passenger - Baggage Security Screening)

In this Scenario we will report the current regulation about security measures on passenger and baggage from the check in point of the departure airport to the baggage reclaim at the arrival airport.

There will be a focus about the new technologies for passenger check (such as body scanner) and about the passenger-baggage reconciliation procedure.

Security measures start from the architectural design and building of the Airport facilities and cover all main aspects of an Airport daily activity.

Airport planning requirements

Regulation 300/2008 [6] requires implementation of the common basic standards (set out in the Annex of the Regulation) when designing and constructing new airport facilities or altering existing airport facilities. At airports the following areas shall be established:

1. landside;
2. airside;
3. security restricted areas; and
4. critical parts of security restricted areas[1].

Airport security programme

Every airport operator shall draw up, apply and maintain an airport security programme. This programme describes the methods and procedures which are to be followed by the airport personnel in order to comply with all the applicable EC regulations and the national civil aviation security programme of the Member State in which the airport is located.

[1] Closer description of critical parts of security restricted areas is given in Regulation 185/2010.

The security programme shall include internal quality control provisions describing how compliance with these methods and procedures is to be monitored by the airport operator. The airport security programme shall be submitted to the appropriate authority, which has to approve it. In the following some excerpts and/or rephrasing of the above mentioned EC Regulations.

Implementation of security measures
Unless otherwise stated or unless the implementation of screening is ensured by an authority or entity, an airport operator should ensure the implementation of the measures set out in the doc [6] and described in details below.

Security controls
Supplies intended to be sold or used in security restricted areas of airports, including supplies for duty-free shops and restaurants, should be subjected to security controls in order to prevent prohibited articles from being introduced into these areas.

Persons
Persons entering airside or security restricted areas of an airport can be classified as follows:

1. passengers;
2. persons other than passengers: airport personnel, airlines personnel or personnel of entities providing services to an airport (ATC, construction, maintenance, catering, etc.).

Passengers and cabin baggage
The requirements for checking passengers and their cabin baggage in accordance to the valid EU regulations are as follows:

1. All originating, transfer and transit passengers and their cabin baggage shall be screened in order to prevent prohibited articles from being introduced into security restricted areas and on board an aircraft.
2. Transfer passengers and their cabin baggage may be exempted from screening, if:
    a. they arrive from a Member State, unless the Commission or that Member State has provided information that those passengers and their cabin baggage cannot be considered as having been screened to the common basic standards; or
    b. they arrive from a third country where the security standards applied are recognised as equivalent to the common basic standards.

    Transit passengers and their cabin baggage may be exempted from screening, if:
    a. they remain on board the aircraft; or
    b. they do not mix with screened departing passengers other than those who board the same aircraft; or
    c. they arrive from a Member State, unless the Commission or that Member State has provided information that those passengers and their cabin baggage cannot be considered as having been screened to the common basic standards; or

d. they arrive from a third country where the security standards applied are recognised as equivalent to the common basic standards.

These above-mentioned points are usually addressed by design of terminal, were transfer and transit passengers are physically separated from the landside. If these passengers leave the airside and go to landside at transfer/transit airport then they need to go through security check again as other regular departing passengers.

Screened departure passengers and their cabin baggage shall be protected from interference and these passengers shall not mix with arriving passengers from a State (either a Member State or a third country) which cannot be considered as compliant with standards equivalent to the common basic standards of EU States. This requirement is also fulfilled by the design of airside part of airport terminals.

It is noteworthy that apart from regular screening and checks the security personnel is also trained to:

1. search for unattended baggage/bags/packages and react appropriately when such item is found;
2. react when they hear certain keywords such as “bomb”, “firearm”, “weapon”, etc.

Whenever unscreened persons may have had access to critical parts of security restricted areas, a full security search of those parts shall be carried out. This requirement does not relate to unscreened staff escorted by screened person [7].

Screening of passengers and cabin baggage

Screening of passengers is aimed at detection of articles which are prohibited at security restricted areas and the cabin of an aircraft. These articles are classified into the following categories [7]:

1. guns, firearms and weapons (e.g. pistols, replicas, toy guns, etc);
2. pointed/edged weapons and sharp objects (e.g. axes, darts, ice skates, etc);
3. blunt instruments (e.g. baseball bat, golf club, hockey stick, etc.);
4. explosives and flammable substances;
5. chemical and toxic substances;
6. liquids.

Despite these articles are prohibited, certain exceptions can apply for example, liquids can be carried on board an aircraft for medical purposes or a special dietary requirements. In addition, a passenger may be granted an exemption for any article mentioned in Regulation 820/2008 [8] provided that:

1. The appropriate authority has been informed in advance and given consent that the article may be carried; and
2. The captain of the aircraft has been informed about the passenger and the prohibited article he/she is carrying.

Where appropriate the prohibited article shall be placed in secure conditions.

Screening procedure for passengers

According to the Regulation 272/2009 [9] the following methods of screening of persons are allowed (individually or in combination, as a primary or secondary means and under defined conditions):

1. Hand Search – detailed provisions for a hand search are laid down in [7] and in Commission Decision (CD(2008) 4333) [10]. and are described below;

2. Walk-Through Metal Detection (WTMD) equipment – is able to detect and to indicate by means of an alarm certain specified metallic items, both individually and in combination. The alarm is visual and audible and noticeable at a range of 2 m at minimum. The visual alarm shall give an indication of the strength of signal detected by the WTMD. WTMD generates signal on a percentage of persons passing through the WTMD who did not cause an alarm. It is possible to set the percentage. WTMD is also able to count the number of persons screened, excluding any person that passes through the WTMD in the opposite direction and count the number of alarms (plus to calculate ratio of alarms to screened persons in %). WTMD is regularly tested (at some airports it may be every day) and calibrated (approximately once a month);
3. Hand-Held Metal Detection (HHMD) equipment;
4. Explosive Detection Dogs;
5. Explosive Trace Detection (ETD) equipment.

Before screening, coats and jackets of passengers shall be taken off and shall be screened as cabin baggage. Passengers shall be screened by a hand search or WTMD equipment. Where the screener cannot determine whether or not the passenger is carrying prohibited articles, the passenger shall be denied access to security restricted areas or rescreened to the screener's satisfaction.

When a hand search is performed it shall be carried out so as to reasonably ensure that the person is not carrying prohibited articles. When WTMD equipment alarms, the cause of the alarm shall be resolved. Hand-held metal detection (HHMD) equipment may only be used as a supplementary means of screening. It shall not replace the requirements of a hand search.

Where a live animal is permitted to be carried in the cabin of an aircraft, it shall be screened either as a passenger or as cabin baggage.

The appropriate authority (e.g. CAA) may create categories of passengers that, for objective reasons, shall be subject to special screening procedures or may be exempted from screening. The Commission shall be informed of the categories created.

The screening of passengers is also be subject to the additional provisions laid down in a Commission Decision (CD(2008) 4333 [10]).

Not less than 10% of passengers who caused the WTMD equipment to alarm shall be searched by hand. However, airport can follow stricter procedures and according to our information at some airports all such passengers are searched by hand.

Not less than 10% of passengers who did not cause the WTMD equipment to alarm shall be searched by hand. This shall be measured for each 100 passengers passing through the WTMD equipment. Notwithstanding the previous, hand searches shall be carried out on a continuous random basis.

In addition CCTV cameras are used in airports as a preventive and monitoring measures. The usage of such technologies should always be compliant with the 95/46/EC European Directive [11], currently under rediscussion at the European Parlament.

Screening procedure for cabin baggage

Before screening, portable computers and other large electrical items shall be removed from cabin baggage and shall be screened separately. Any bag subject to screening by x-ray equipment that is found to contain a large electrical item shall be screened again with the item removed from the bag and the item screened separately.

All liquids shall be presented at screening points for examination. Before screening, liquids, aerosols and gels' (LAGs) shall be removed from cabin baggage and shall be screened separately, unless the equipment used for the screening of cabin baggage is also capable of screening multiple closed LAG containers inside baggage.

Where LAGs have been removed from cabin baggage, the passenger shall present:

1. all LAGs in individual containers with a capacity not greater than 100 millilitres or equivalent in one transparent re-sealable plastic bag of a capacity not exceeding 1 litre, whereby the contents of the plastic bag fit comfortably and the bag is completely closed; and
2. other LAGs separately.

Cabin baggage shall be screened by:

1. a hand search; or
2. x-ray equipment; or
3. explosive detection systems (EDS) equipment. EDS is either a Primary Explosive Detection Systems (PEDS) or Explosive Device Detection System (EDDS). EDS is able to detect and to indicate higher individual quantities of explosive material contained in baggage. EDS is regularly tested.

Where the screener cannot determine whether or not the cabin baggage contains any prohibited articles, it shall be rejected or rescreened to the screener's satisfaction.

A hand search of cabin baggage shall consist of a manual check of the baggage, including its contents, as to reasonably ensure that it does not contain prohibited articles.

Where x-ray or EDS equipment is used, each image shall be viewed by the screener. All alarms shall be resolved to the satisfaction of the screener so as to reasonably ensure that no prohibited articles are carried into the SRA or on board an aircraft.

Where x-ray or EDS equipment is used, any item whose density impairs the ability of the screener to analyse the contents of the cabin baggage shall be taken out of the baggage. The bag shall be screened again and the item shall be screened separately as cabin baggage.

Explosive detection dogs and explosive trace detection (ETD) equipment may only be used as a supplementary means of screening.

The appropriate authority may create categories of cabin baggage that, for objective reasons, shall be subject to special screening procedures or may be exempted from screening. The Commission shall be informed of the categories created.

The appropriate authority may allow a diplomatic bag to be exempted from screening or to be subjected to special security procedures provided that the requirements of the Vienna Convention on Diplomatic Relations are met.

Screening of liquids, aerosols and gels (LAGs)

LAGs shall be screened by:

1. x-ray equipment;
2. explosive detection systems (EDS) equipment;
3. explosive trace detection (ETD) equipment;
4. chemical reaction test strips; or
5. bottled liquid scanners.

Tasting or testing on the skin may be used as a supplementary means of screening.

LAGs carried by passengers may be exempted from screening if the LAG is:

1. in individual containers with a capacity not greater than 100 millilitres or equivalent in one transparent re-sealable plastic bag of a capacity not exceeding 1 litre, whereby the contents of the plastic bag fit comfortably and the bag is completely closed; or
2. to be used during the trip and is either required for medical purposes or a special dietary requirement, including baby food. When requested to do so the passenger shall provide proof of authenticity of the exempted liquid; or
3. obtained airside beyond the point where boarding passes are controlled from outlets that are subject to approved security procedures as part of the airport security programme, on condition that the liquid is packed in a bag that is both tamper evident and displays satisfactory proof of purchase at that airport on that day; or
4. obtained in the security restricted area from outlets that are subject to approved security procedures as part of the airport security programme; or
5. obtained at another Community airport, on condition that the liquid is packed in a bag that is both tamper evident and displays satisfactory proof of purchase at airside at that airport on that day; or
6. obtained on board an aircraft of a Community air carrier, on condition that the liquid is packed in a bag that is both tamper evident and displays satisfactory proof of purchase on board that aircraft on that day.

Staff recruitment, background checks and training

Persons implementing, or responsible for implementing, screening, access control or other security controls shall be recruited, trained and, where appropriate, certified so as to ensure that they are suitable for employment and competent to undertake the duties to which they are assigned. These persons shall also successfully complete background check before identification card authorising unescorted access to security restricted areas is issued to them.

Persons other than passengers requiring access to security restricted areas shall receive security training (theoretical, practical and/or on-the-job), before either an airport identification card or crew identification card is issued. These persons shall also successfully complete background check before identification card authorising unescorted access to security restricted areas is issued to them.

Hold Baggage

For hold baggage the following procedures apply:

1. All hold baggage shall be screened prior to being loaded onto an aircraft in order to prevent prohibited articles from being introduced into security restricted areas and on board aircraft.
2. Transfer hold baggage may be exempted from screening, if:
    a) it arrives from a Member State, unless the Commission or that Member State has provided information that this hold baggage cannot be considered as having been screened to the common basic standards; or
    b) it arrives from a third country where the security standards applied are recognised as equivalent to the common basic standards.
3. Transit hold baggage may be exempted from screening if it remains on board the aircraft.

Hold baggage has to be protected from unauthorised interference from the point at which it is screened.

Baggage reconciliation

An air carrier shall, during the boarding process, ensure that a passenger presents a valid boarding card or equivalent corresponding to the hold baggage that was checked in.

An air carrier shall ensure that there is a procedure in place to identify hold baggage of passengers who did not board or left the aircraft before departure.

If the passenger is not on board the aircraft, the hold baggage corresponding to his boarding card or equivalent shall be considered as unaccompanied.

An air carrier shall ensure that each item of unaccompanied hold baggage is clearly identifiable as authorised for transport by air.

Left luggage

Some airports provide a service of storing left luggage. Left luggage should be screened in a similar way as cabin or hold baggage in case staffed office is used for providing this service. If automatic left luggage lockers are used, then ideally these should be excluded from public areas. Further guidance on automatic left luggage lockers is in Annex IV-2-E of ECAC Doc 30 [4].

Summary of screening methods

In accordance with the Regulation 272/2009, the following methods of screening of baggage, cargo, mail and other goods are allowed (individually or in combination, as a primary or secondary means and under defined conditions):

1. For the screening of cabin baggage, items carried by persons other than passengers, air carrier mail and air carrier materials except when to be loaded into the hold of an aircraft, in-flight supplies and airport supplies:
   a) hand search;
   b) visual check;
   c) x-ray equipment;
   d) explosive detection systems (EDS) equipment;
   e) explosive detection dogs; and
   f) explosive trace detection (ETD) equipment.
2. For the screening of liquids, gels and aerosols:
   a) tasting or testing on the skin;
   b) visual check;
   c) x-ray equipment;
   d) explosive detection systems (EDS) equipment;
   e) explosive detection dogs;
   f) explosive trace detection (ETD) equipment;
   g) chemical reaction test strips; and
   h) bottled liquid scanners.
3. For the screening of hold baggage, cargo and mail as well as air carrier mail and air carrier materials to be loaded into the hold of an aircraft:
   a) hand search;
   b) visual check;

c) x-ray equipment;
d) explosive detection systems (EDS) equipment;
e) explosive detection dogs;
f) explosive trace detection (ETD) equipment; and
g) simulation chamber.

Research Questions
Since the deployment of a new security measure is costly, this means that the incentive for airports to engage in security investment may not coincide with the government's desire for them to do so. This observation raises the question regarding the behavior of stakeholders in airport networks against security threats and the adoption of security measures. In this scenario, we would like to investigate how the deployment of different security measures that were identified in WP1 will have an impact on heterogeneous airports in two types of airport networks (i.e., hub & spoke and point to point). That is, the main objectives of the study would be to identify how the deployment of security measures, e.g., baggage reconciliation, full body scanner or training programs will impact on configuration of different types of airports and different type of threats.
Two main research questions are introduced:

(1) Airports' Networks

Hubs, spoke and low cost airports: what is the difference from security effectiveness, security cost and decision perspective in implementing new security measures?
Cost sharing, investments, airport profit margin how do they affect risk management and security measures implementation?
How can the risk perception of passengers and airport operators and social acceptance of security measures be modeled and quantified?

(2) New Threats

New security measures and emerging threats, what is the balance between them in terms of cost and technology, security gain and risk perception of passengers?
What are the main features of new kind of weapons that are used to attack the airport or the airplane? And what the possible countermeasures?

During year two we will analyse and model the implementation of different Security Measures in various Airport in order to understand if there are major differences between small and big European Airports, how costs and revenues are split among different stakeholders, how it is possible to optimise the selection and implementation of Security Measures taking into account risks, economical and societal constraints.
Moreover, we will try to understand if and how current Security Measure can properly detect new security threats and malicious attacks (innovative IT based multiple attacks and/or bio-terrorism) and effectively mitigate them.

4.2.2 Training for Airport Personnel

Generally, the common basic standards about Security Training for Airport Personnel in Europe are laid down by the Commission Regulation (EU) No 185/2010 [7] of March 2010.

Firstly, Section 11.1.4 of the Regulation describes the requirements which a background and pre-employment check shall fulfill (in accordance with Community rules, national rules and national civil aviation security programmes).
In Europe, background or pre-employment check shall be completed before the person undergoes any security training involving access to information which is not publicly available.
It is also defined that persons being recruited to implement security controls shall have the mental and physical abilities to carry out their designated tasks effectively and shall be made aware of the nature of these requirements at the outset of the recruitment process. These abilities shall be assessed during the recruitment process and before completion of any probationary period.
The contents of the aviation security training in Europe are regulated by the section 11.2 of the Regulation which defines:

- general training obligations,
- basic training,
- job specific training for persons implementing security controls,
- specific training for persons directly supervising persons implementing security controls (supervisors),
- specific training for persons with general responsibility at national or local level for ensuring that a security programme and its implementation meet all legal provisions (security managers) and
- training of persons other than passengers requiring unescorted access to security restricted areas.

General Security Training Obligations
Persons shall have successfully completed relevant training before being authorised to implement security controls unsupervised.
Training of persons performing tasks shall include theoretical, practical and on-the-job training elements.
The content of courses shall be specified or approved by the appropriate authority before:

- an instructor delivers any training required under Regulation (EC) No 300/2008 [6] and its implementing acts; or
- a computer based training course is used in order to meet the requirements of Regulation (EC) No 300/2008 [6] and its implementing acts.

Computer based training may be used with or without the support of an instructor or coach.
Training records shall be kept for all persons trained for at least the duration of their contract.

Basic Training
Basic training of persons performing security tasks shall result in the following competencies:

(a) knowledge of previous acts of unlawful interference with civil aviation, terrorist acts and current threats
(b) knowledge of the legal framework for aviation security;

(c) knowledge of the objectives and organisation of aviation security, including the obligations and responsibilities of persons implementing security controls;
(d) knowledge of access control procedures;
(e) knowledge of identification card systems used at the airport;
(f) knowledge of procedures for challenging persons and of circumstances in which persons should be challenged or reported;
(g) knowledge of reporting procedures;
(h) ability to identify prohibited articles;
(i) ability to respond appropriately to security related incidents;
(j) knowledge of how human behaviour and responses can affect security performance; and
(k) ability to communicate clearly and confidently.

Job Specific Training for Persons implementing Security Controls

Job specific training of persons implementing screening of persons, cabin baggage, items carried and hold baggage shall result in the following competencies:

(a) understanding of the configuration of the screening checkpoint and the screening process;
(b) knowledge of how prohibited articles may be concealed;
(c) ability to respond appropriately to the detection of prohibited articles;
(d) knowledge of the capabilities and limitations of security equipment or screening methods used;
(e) knowledge of emergency response procedures;
(f) interpersonal skills, in particular how to deal with cultural differences and with potentially disruptive passengers;
(g) knowledge of hand searching techniques;
(h) ability to carry out hand searches to a standard sufficient to reasonably ensure the detection of concealed prohibited articles;
(i) knowledge of exemptions from screening and special security procedures;
(j) ability to operate the security equipment used;
(k) ability to correctly interpret images produced by security equipment; and
(l) knowledge of protection requirements for hold baggage.

Training of persons implementing screening of cargo and mail shall result in the following competencies:

(a) knowledge of previous acts of unlawful interference with civil aviation, terrorist acts and current threats;
(b) awareness of the relevant legal requirements;
(c) knowledge of the objectives and organisation of aviation security, including the obligations and responsibilities of persons implementing security controls in the supply chain;
(d) ability to identify prohibited articles;
(e) ability to respond appropriately to the detection of prohibited articles;
(f) knowledge of the capabilities and limitations of security equipment or screening methods used;
(g) knowledge of how prohibited articles may be concealed;
(h) knowledge of emergency response procedures;

(i) knowledge of protection requirements for cargo and mail; and
(j) where the person's designated tasks so require:
a. knowledge of screening requirements for cargo and mail, including exemptions and special security procedures;
b. knowledge of screening methods appropriate for different types of cargo and mail;
c. knowledge of hand searching techniques;
d. ability to carry out hand searches to a standard sufficient to reasonably ensure the detection of concealed prohibited articles;
e. ability to operate the security equipment used;
f. ability to correctly interpret images produced by security equipment; and
g. knowledge of transportation requirements.

Training of persons implementing screening of air carrier mail and materials, inflight supplies and airport supplies shall result in the following competencies:
(a) knowledge of previous acts of unlawful interference with civil aviation, terrorist acts and current threats;
(b) awareness of the relevant legal requirements;
(c) knowledge of the objectives and organisation of aviation security, including the obligations and responsibilities of persons implementing security controls in the supply chain;
(d) ability to identify prohibited articles;
(e) ability to respond appropriately to the detection of prohibited articles;
(f) knowledge of how prohibited articles may be concealed;
(g) knowledge of emergency response procedures;
(h) knowledge of the capabilities and limitations of security equipment or screening methods used; and
(i) where the person's designated tasks so require:
a. knowledge of hand searching techniques;
b. ability to carry out hand searches to a standard sufficient to reasonably ensure the detection of concealed prohibited articles;
c. ability to operate the security equipment used;
d. ability to correctly interpret images produced by security equipment; and
e. knowledge of transportation requirements.

Specific training of persons performing vehicle examinations shall result in the following competencies:
(a) knowledge of the legal requirements for vehicle examinations, including exemptions and special security procedures;
(b) ability to respond appropriately to the detection of prohibited articles;
(c) knowledge of how prohibited articles may be concealed;
(d) knowledge of emergency response procedures;
(e) knowledge of vehicle examination techniques; and
(f) ability to carry out vehicle examinations to a standard sufficient to reasonably ensure the detection of concealed prohibited articles.

Specific training of persons implementing **access control** at an airport as well as surveillance and patrols shall result in the following competencies:

(a) knowledge of the legal requirements for access control, including exemptions and special security procedures;
(b) knowledge of access control systems used at the airport;
(c) knowledge of authorisations, including identification cards and vehicle passes, providing access to airside areas and ability to identify those authorisations;
(d) knowledge of procedures for patrolling and for challenging persons and of circumstances in which persons should be challenged or reported;
(e) ability to respond appropriately to the detection of prohibited articles;
(f) knowledge of emergency response procedures; and
(g) interpersonal skills, in particular how to deal with cultural differences and with potentially disruptive passengers.

Training of persons implementing aircraft security searches shall result in the following competencies:

(a) knowledge of the legal requirements for aircraft security searches;
(b) knowledge of the configuration of the type(s) of aircraft on which the person is to implement aircraft security searches;
(c) ability to identify prohibited articles;
(d) ability to respond appropriately to the detection of prohibited articles;
(e) knowledge of how prohibited articles may be concealed; and
(f) ability to implement aircraft security searches to a standard sufficient to reasonably ensure the detection of concealed prohibited articles.

Training of persons implementing aircraft protection shall result in the following competencies:

(a) knowledge of how to protect and prevent unauthorised access to aircraft;
(b) knowledge of procedures for sealing aircraft, if applicable;
(c) knowledge of identification card systems used at the airport;
(d) knowledge of procedures for challenging persons and of circumstances in which persons should be challenged or reported; and
(e) knowledge of emergency response procedures.

Training of persons implementing baggage reconciliation shall result in the following competencies:

(a) knowledge of previous acts of unlawful interference with civil aviation, terrorist acts and current threats;
(b) awareness of the relevant legal requirements;
(c) knowledge of the objectives and organisation of aviation security, including the obligations and responsibilities of persons implementing security controls;
(d) ability to respond appropriately to the detection of prohibited articles;
(e) knowledge of emergency response procedures;
(f) knowledge of passenger and baggage reconciliation requirements and techniques; and

(g) knowledge of protection requirements for air carrier materials used for passenger and baggage processing.

Training of persons implementing security controls for cargo and mail other than screening, or having access to identifiable air cargo or identifiable air mail, shall result in the following competencies:

(a) knowledge of previous acts of unlawful interference with civil aviation, terrorist acts and current threats;
(b) awareness of the relevant legal requirements;
(c) knowledge of the objectives and organisation of aviation security, including the obligations and responsibilities of persons implementing security controls in the supply chain;
(d) knowledge of procedures for challenging persons and of circumstances in which persons should be challenged or reported;
(e) knowledge of reporting procedures;
(f) ability to identify prohibited articles;
(g) ability to respond appropriately to the detection of prohibited articles;
(h) knowledge of how prohibited articles may be concealed;
(i) knowledge of protection requirements for cargo and mail; and
(j) knowledge of transportation requirements, if applicable.

Specific Training for Supervisors

Specific training of supervisors shall, in addition to the competencies of the persons to be supervised, result in the following competencies:

(a) knowledge of the relevant legal requirements and how they should be met;
(b) knowledge of supervisory tasks;
(c) knowledge of internal quality control;
(d) ability to respond appropriately to the detection of prohibited articles;
(e) knowledge of emergency response procedures;
(f) ability to provide mentoring and on-the-job training and to motivate others; and
(g) where the person's designated tasks so require:
    a. knowledge of conflict management; and
    b. knowledge of the capabilities and limitations of security equipment or screening methods used.

Specific Training for Security Managers

Specific training of security managers shall result in the following competencies:

(a) knowledge of the relevant legal requirements and how they should be met;
(b) knowledge of internal, national, Community and international quality control;
(c) ability to motivate others;
(d) knowledge of the capabilities and limitations of security equipment or screening methods used.

Training Of Persons Other Than Passengers Requiring Unescorted Access To Security Restricted Areas

Persons other than passengers requiring unescorted access to security restricted areas shall receive security awareness training before being issued with an authorisation granting unescorted access to security restricted areas.

Security awareness training shall result in the following competencies:

(a) knowledge of previous acts of unlawful interference with civil aviation, terrorist acts and current threats;
(b) awareness of the relevant legal requirements;
(c) knowledge of the objectives and organisation of aviation security, including the obligations and responsibilities of persons implementing security controls;
(d) understanding of the configuration of the screening checkpoint and the screening process;
(e) awareness of access control and relevant screening procedures;
(f) knowledge of airport identification cards used at the airport;
(g) knowledge of reporting procedures; and
(h) ability to respond appropriately to security related incidents.

Each person undergoing security awareness training shall be required to demonstrate understanding of all subjects referred to in section 10.7 before being issued with an authorisation granting unescorted access to security restricted areas.

Recurrent Training

Section 11.4.1 of the Regulation defines the requirements for recurrent training of persons operating x-ray or EDS equipment. According to the section 11.4.2 of the Regulation, the persons performing tasks as listed under point 11.2 of the Regulation other than those referred in point 11.4.1 of the Regulation shall undergo recurrent training at a frequency sufficient to ensure that competencies are maintained and acquired in line with security developments.

Research Questions

Among the vast number, overlapping reach, and variable nature of the security measures in the Airport domain, the training of personnel is part of the control areas mentioned in internationally recognized frameworks, such as:

- the ISO/IEC 27002:2013 [12] and
- the NIST SP 800-53 rev.3 [13]

These two most widespread and referenced frameworks are seleceted as best practice in this field and represent a concrete step towards completeness.

Both frameworks identify families of controls with the ISO standard counting 14 groupings and the NIST standard counting 18. Both standards cover the whole spectrum of security measures looking at control families from the lens of measure’s functionalities and identify five security control areas (SCAs):

- governance and people,
- policy, processes and procedures
- operations,
- technical controls,
- incident response.

The governance and people control area include “security awareness and training” as well as related measures such as “enforcement of disciplinary measures” and “preventive security assessment on employees and 3rd parties”.

Impact and relevance of training interventions, including awareness raising, empowerment and introduction of new security procedures, have been recognized throughout the stakeholders needs identification activities (see Table 2).

We will analyse and model the selection and delivery of Training in different Airports in order to understand:

- if there are major differences between small and big European Airports,
- how costs of basic and recurrent Training are split among different stakeholders,
- how it is possible to optimise the selection of different Training solutions (classroom courses, e-learning, on the job training, etc.) taking into account economical and social constraints from an employees perspective.
- if and how current Training can properly detect new security threats and malicious attacks (e.g. innovative IT based multiple attacks and/or bio-terrorism)
- if more focus on Technology, Human Factors and Organizational aspects and/or ‘ad-hoc’ training for profiling would be needed.

The WP1 study on the Training scenarios will aim at developing a model that can investigate appropriate training strategies. In order to do this, we will use both an economic approach (see Section 5.1) and a behavioral approach (see [14] for further details). Regarding a behavioral approach, for example, since one of the most important aspects of security training is to increase the ability of employees to respond and act upon unexpected and unpredictable events, we prepared the following preliminary questions which encompass personal perspective, understanding, preparedness, and exercise of authority and information sharing:

- Personal Perspectives:
    - Is it worth to worry about emerging threats?
    - Do you think emerging threats can be dealt with existing security measures?
- Preparedness
    - Does your organization have a training program for coping with emerging threats? (e.g., devising the tactics to address them and identifying key officials, etc)
    - Does your organization have procedures (or manual, guide book) for identifying emerging threats and for dealing with these threats?
    - Does your organization have early viable warning systems when an unknown possible threat is identified?
- Exercise of Authority and Information sharing
    - Does your organization have skilled personnel responsible to assess a potentially dangerous device? If yes, who is in charge for this?
    - Does your organization have the chain-of-command or lines-of-authority whom to be contacted in case of the finding of emerging threats?

- Does your organization have a clear communication path for information sharing internally (between workers) in case of unexpected events caused by new threats?
- Does your organization have a clear communication path for information sharing to other organizations (e.g., police or military personnel) in case of unexpected events caused by new threats?

In this study, we also want to investigate whether there is some effect (say, "social ripple effect"). For example, in case where a new threat is found, the government may employ security measures against the new threat without proper evaluation of the threat. That is, the government may invest in security measures not because they are really dangerous but because media and public opinion directly request for it. In the interview, we will try to identify whether there is such type of an effect against new threats.

4.3 Airport Security Scenarios

The following describes a case study which retains most of the essence that an airport operator (AO) needs to face as far as security is concerned. Details and data of Anadolu Airport (henceforward AA) are fictitious to preserve confidentiality (and for security reasons).

4.3.1 Description of AA Airport

The AA airport is operated by an Airport Operator with certification of Directorate General of Civil Aviation (National Civil Aviation Authority). The airport was established in University campus.

AA international airport is located in medium sized city which has developing potential with two big universities and industrial region of aviation companies. Airport has single runway and it's air traffic includes international, regional airline and flight training operations with small density of general aviation operations.

AA airport has the international and domestic flights with high frequency flight training operations. The aerodrome control service (Air Traffic Control (ATC) Tower), AIM, airside operations, Rescue-Fire Fighting (RFF), emergency services and aircraft maintenance service are provided by University technical personnel. The terminal control (TRACON) service is provided by military ATC which is located in neighbor air base of same city. Custom service is provided by local custom officers.

Airlines has office in the terminal where provides ticketing for airline companies. Additionally, an airline provides check-in, boarding, baggage, ramp services, balance, de/anti-icing, APU, ASU, marshaling ext. for itself and service requesting flights operators.

The fuelling and re-fuelling services are provided by different companies.

4.3.2 AA Airport Security Structure and Stakeholders

The Civilian Authority of AA airport is the city Governor assigned by national law. The governor empowers one of his Assistant Governors to manage airport security operations and official permissions. For instance, any research study should be presented to governor and should be approved by governor first.

Airport Security Commission (ASC): Airport security commission is the decision-making body which meets in council every month about AA airport security issues. The commission consists of executive authorized people from all stakeholders related to airport. ASC members are Assistant Governor (Chairman), the airport police chief, private security chief, custom officer, airport manager, the University Representative (responsible for airport operations and represents university rector), Airline representative and emergency service member.

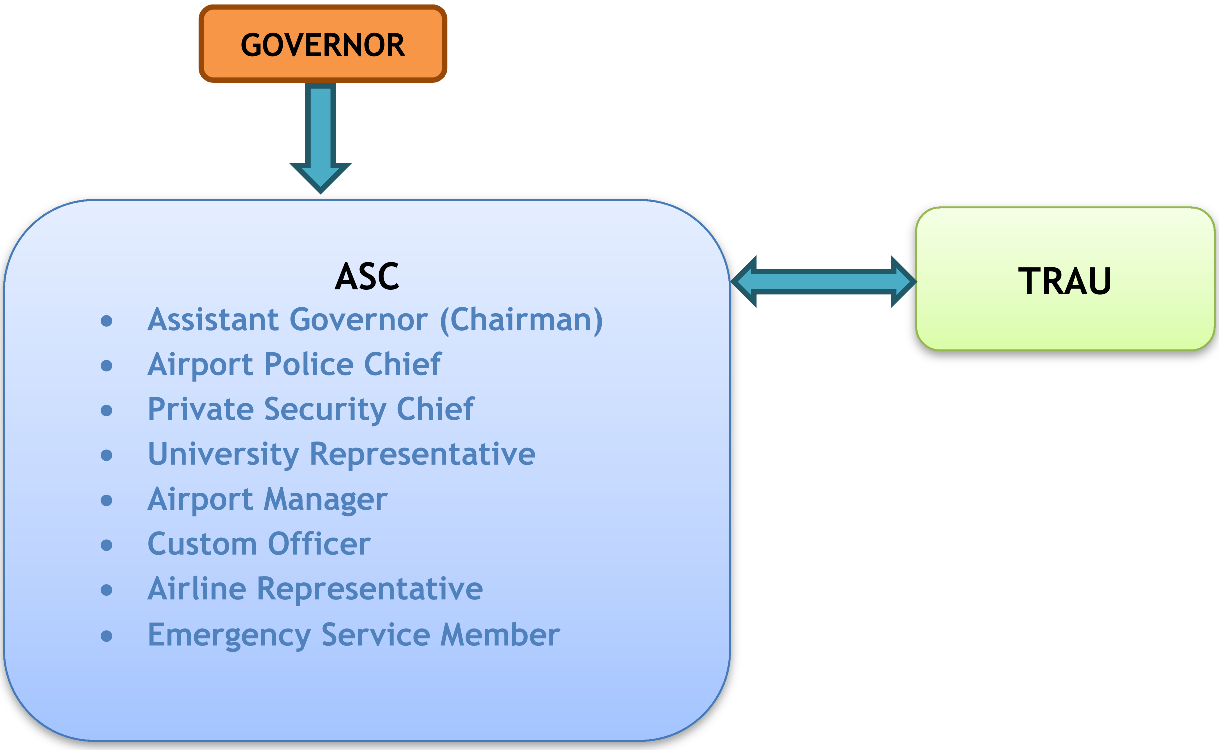

Figure. 4. Relation between stakeholders about AA airport security.

Training, Research and Auditing Unit (TRAU): The unit was established by recommendation on ICAO Annex 17 [3], Chapter 3 and meets in council in every week. The main objectives of this unit are to compose airport security program by presenting to ASC approval and to provide useful information and recommendations for the ASC. The unit members consist of the representatives from the secondary level positions of ASC members.

Given the situation, the management of AA airport can create a budget when required for the security needs during the operation year.

4.3.3 Scenario Description

The management of AA airport is worried about recent changes in security trend within the system, specially taking into account changes in the socio-economic background and risk perception about airport security.
There are different design approaches about positioning of Air Traffic Management ATM facilities in the airports around the world. Some of them take a place in the airside where is well secured, some are around/in the terminal buildings with some unsecure check points/barriers.

It is especially concerned with the global risk perception about any terrorist attack to airports and air traffic management systems within all related resources. Aviation security environment is worried about weak points in the information communication technology in ATM. Hackers can interrupt or use these systems for their goals and can create conflictions between airplanes and obstacles[2]. This perception could increase highest level when the attackers reach up to ATC facilities and Air Traffic Controllers by using weak points in security checks at airports to get into. ATM operations stand in the centre of the airport operations. ATM related security incidents can create flight safety disasters and damages on the high cost facilities, equipment and airplanes.

When any potential risks occurred at the airport and related operations, security perception of people can be damaged as air travel is hazardous. This image can create additional security barriers and investments/costs for the airports and ATM operations. Consequently it means that new barriers for the passengers and airport users. On the other hand it means new workload reflections for the security people working at the airport.

Unlawful Access to the Tower and Interference to ATC Operations

Scenario: The AA airport ATC Tower is attached to the terminal building and its gate is located in the main lounge of terminal. An attacker person among the passengers can plan to enter tower and to take hold of air traffic controllers before or during the flight control operations. After the first security checks he/she could find an opportunity for tower entrance gate which is remote controlled camera display check by air traffic controllers. He/she goes up to the tower and could capture controllers. He/she can use all radio and telephone communication aids in tower to pass his message.

Impacts: Crisis for air traffic operations in the air field and airspace. Flight safety negatively affected and air traffics should be diverted to the other ATC unit or air field.

[2] "Hackers Attack to ATC", http://abcnews.go.com/US/story?id=95993&page=1; "Air Traffic System Vulnerable to Cyber Attack", http://www.newscientist.com/article/mg21128295.600-air-traffic-system-vulnerable-to-cyber-attack.html; "Laser Attacks", http://www.caa.co.uk/docs/33/SafetyNotice2012005.pdf . "Host Systems", http://om.adsgroup.org.uk/directorydetail.aspx?OrganisationId=2433&directorycode=6331&infocode=ORG_DIR&returnpage=1&resultsperpage=10&cstype=BAG

During the first crisis session pilots and other related operators couldn't understand the happenings. Pilots have to manage their flights and their operational safety.

- All flight operations are cancelled or diverted to alternative airfields. Beside the safety and security impacts the cancellation cost can be enormous with the connected national and international flights and airports/airspace.
- Media can inform people immediately about the situation. This can cause new crisis around the airport facilities and operators.
- Negative security perception for airport users. As a result of this interference people's image can be affected negatively who are travelling by air.

Agents involved: AA Airport police and Private security, Air Traffic Controllers, Pilots and terminal stuff.

Perpetrator: Somebody who is a member of any ethnic/politic body.

Countermeasures: Security checks, Cameras.

Stakeholders involved: Depending on the situation following stakeholders could be involved for the crisis management. Airport management, Special Police Forces, Governor, related ATC units, neighbour airports, National Navigation Service Provider (ANSP), National Civil Aviation Authority, Eurocontrol, related Military ATC Units, Ministry of Interior, Ministry of Transportation.

4.3.4 Research Questions

ATM related scenario is not common threat for airport security. For this reason operational and high level stakeholders are considered unprepared for every airports. Since some ATC units in the airport are located in airside, its security risk may not be well covered by the stakeholders. In this scenario study, the importance of the ATM security is emphasized and the awareness of the stakeholders will be examined. For this reason, scenario related high level and operational level research questions were developed to have awareness level and attention of airport security stakeholders.

High Level questions:

- What is the role of ATM operations in airport security?
- All operational units are well secured in airports?
- What is the risk level of any attack to the ATM facilities in the airport?
- How is the security awareness/culture for airport employees including critical positions like air traffic controllers?
- How any attack to the ATM facilities could be resulted?
- Are there any simulations or security plans covering this threat?
- How the coordination is managed with the stakeholders in any crisis?

Operational level questions:

- How is the likelihood of any attack to the ATM facilities in your airport?
- What is your role in any occurrence related this scenario?
- Do you know your responsibilities in that situation?

- Did you have any security training for this situation?
- Do you consider that any attack to ATM facilities is not possible?
- How do you consider about results and effects of any attack to ATM facilities in your airport?

As it can be seen above training and risk management efforts will be identifying to improve security perception and awareness for other important airport operations which are very critical for all aviation system.

5. Modelling the Airport Case Study

In this Section the structure of the problems posed by the domain and the modelling methodologies applied by WP5 and WP6 partners are introduced. The description below is just a very high-level introduction to the modelling approaches applied to the Airport Case Study. Details of the WP5 and WP6 models are described in D5.1, D5.2 and D6.1 deliverables.

5.1 WP5 Adversarial Risk Analysis approach

5.1.1 Problem Statement

In general, the security-related decision-making processes follow different steps from the identification and detection of a problem to the application of security measures and follow-ups. Specifically for the airport case study, the authorities are concerned with terrorist threats against the installations, security personnel and other staff and/or passengers. As a way to mitigate, as much as possible, (ideally, to zero occurrence rate) the impact of such terrorists menace, some procedures that airport authorities are considering implementing include baggage and passenger security screening, and the airport personnel security training. These and other related measures have considerable associated costs, but by deploying them the authorities expect to deter the actions of the terrorists before they can harm people or damage the fixtures of the airport.
On the other hand, terrorist groups or individuals are more and more organized, prepared, and financially supported to commit their actions in the last years, especially since September 11, 2001 and all the subsequent “terrorist wars” like e.g. Irak or Afghanistan [15], [16], [17], [18], [19], [20], [21], [22], [23]. They are intelligent attackers, usually with a wide knowledge about the defensive measures the target objective is deploying. The terrorists aim at causing as much damage as possible (in the form of casualties, panic feeling by the population, as a way to blackmail Governments or organizations, etc. As such, they can be regarded as expected utility maximizers.

5.1.2 WP5 solution

With regard to the nature of Airport security opponents as intelligent expected utility maximizers the framework of Adversarial Risk Analysis (ARA) is especially suited for facing this kind of problems.
Should the terrorists perform an (to some extent successful) attack, airport authorities may deploy additional preventive or recovery measures, trying to minimize the costs in lives, fixtures, public image, etc. Therefore, they can be regarded as the Defender in the ARA framework and, analogously to the Attacker, they are also expected utility maximizers (maximizing the utility or equivalent to minimize the costs for the Defender).

The model is intended as an initial attempt to capture the particularities of the terrorist threat problem in the airport case study [15], but it is open to future extensions, as e.g. larger airports, with more than one critical installations to be defended, new threats (more than one intelligent attacker), additional countermeasures deployed by different agents (more than one defender), among others.

We model the problem as a particular case of the Sequential Defend-Attack-Defend model; see Section 3.4 of deliverable *D5.1 - Basic Models for Security Risk Analysis* for a description, and whose influence diagram is shown in Figure 6

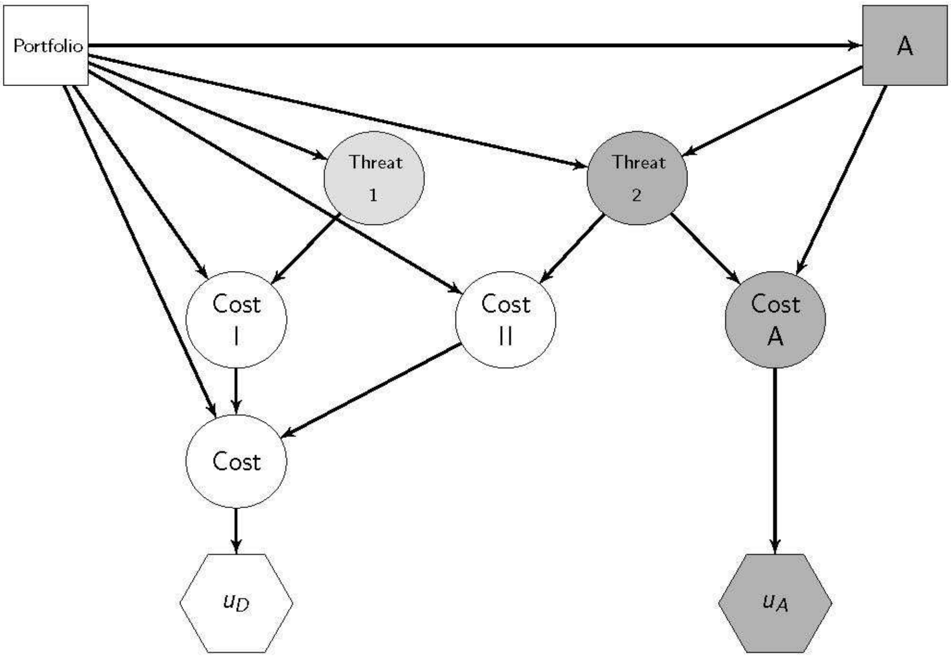

Figure 6 - Coupled influence diagrams for airport case study

In this model, airport authorities (the Defender) would first deploy preventive measures (represented by decision node Portfolio). Then, the terrorist (the Attacker), having observed such decision, would follow a given strategy in order to perform their terrorist attacks (represented by decision node A). Finally, the Defender would try to implement additional measures to mitigate or deter the actions of the terrorists or to recover from their attack (uncertainty node Threat II), whose costs are included in the uncertainty node Cost II. We shall assume that the consequences for the Defender (value node u_D and uncertainty node Cost I in Figure 6) will depend on the effort in implementing their protective and recovery actions and the mitigated result of the terrorist attacks.

On the other hand, the consequences for the Attacker (value node u_A and uncertainty node Cost A in Figure 6) will depend on the effort in developing their terrorist actions and the result of their attack, mitigated by the additional measures eventually implemented by the Defender once the attack has been performed. Besides, we have included another uncertainty node, called Threat I, which accounts for the possibility that there are some other groups or individuals, who are not organized, and whose actions can be regarded as more sparse and random.

Based on the analysis in deliverable *D5.1 - Basic Models for Security Risk Analysis*, the Defender's best strategy would be to choose their optimum portfolio of defensive measures once they have assessed $p_D(A|d_1)$, i.e, their predictive distribution about what strategy will follow the terrorists against each possible set of measures, and later, after observing the eventual attack, choosing additional countermeasures.

We will focus specifically on answering two issues:

1. The design of a particular strategy that an agent can implement. Since an agent's security performance will depend critically on the decisions made by other agents, the agent will choose a security strategy that will maximize its welfare in accordance with the security choices of other agents (e.g., the minimum security investment given the required security level or the most secure portfolio given the security investment level).
2. The design of an adequate security regulation and policy that will govern the relationships and interactions between agents.

5.2 WP6 Economic modelling approach

5.2.1 Problem Statement

Because of interconnected and interdependent security systems of airports, security investments in an airport not only affect its security level but also those of others. This causes inadequacy and inefficiency in airport security investments: in spite of the huge investments in airport security, a residual risk still exists. This interdependence of security is known to cause a positive or negative externality problem. This implies that when there are interdependent security risks, the investments are not adequately allocated to protect systems efficiently and agents will become more vulnerable to security threats.

Due to this situation, the demands for coordination and coalition among stakeholders of airport security have become more crucial: agents involved in airport security need to actively interact with other agents and the security systems in airports need to be coordinated and cooperated adequately.

Since the agents have different sets of constraints and objectives, they have their unique perspectives and economic incentives in mitigating security risks. In order to achieve a global security of the whole systems of airports, however, each stakeholder (i.e. airports, airlines, governments and regulators) should work in a cooperative and interactive manner, and coordinate its security actions with other airports.

5.2.2 WP6 Solution

With regard to the interconnected and interdependent nature of airport security systems an interdisciplinary approach based on economic techniques including a game-tehoretic approach and incentive theory is suitable for studying a broad class of coordination and cooperation issues.

When there is an externality problem mentioned in the previous section, social welfare maximizing choices will not be selected by the players. In this case, some types of regulations and strategies (for example, imposing minimum levels of effort and investment in technological security measures and security training) should be formed to draw social cooperation and ensure a socially optimal outcome. An economic model will allow us to identify regulations and strategies that can incur a socially optimal outcome.

For example, one of the economic techniques we chose to use is a game-theoretic model. This modeling approach uses mathematical techniques for tackling conflict and cooperation issues between players. This approach is particularly useful in studying economic interactions. In the aviation industry, these interactions have varying levels from the regulator at the very top to individual airports and to airport employees at the bottom. The game-theoretic approach will allow us to analyse the interactions among the players and to identify appropriate security policies and strategies which can align the players' incentives well and can incur maximum social welfare. By developing a game-theoretic model, we will identify optimal security regulations and strategies at the pan-European, state and airport levels.

6. Conclusion

In this report we have presented the high level policy and the operational airport security scenarios of WP1 stemming out from the analysis of the Airport Security requirements. The scenarios have been identified and developed in numerous meetings involving a variety of Airport security stakeholders.

The three selected scenarios are:

(1) the *Security Measures* Scenario,
(2) the *Training of Airport Personnel* scenario,
(3) the *Unlawful Access to Tower* Scenario.

These scenarios will be used as a basis to steer the model development and evaluation in real contexts. During the project lifecycle they may be modified according to stakeholders' needs and scientific WPs research interests.
All the three scenarios have been assessed as very relevant both for the airport domain and for the project research activities.

The first scenario offers the opportunity to analyse the bidirectional influence of events occurring at operational level and decisions at policy level.
The second one was considered appropriate and interesting by all the stakeholders that identified improvement of Security Culture as a key issue in airport organisations.
The last scenario describes one of the most widespread threat that affects airport security, having consequences on economic and societal aspects (e.g. due to resonance on media).

Given that the presented scenarios examine the current situation from social and economic parameters, Airport security models aim to be adapted to airports of different sizes.

In particular

- Do the current security regulations adequately and appropriately ensure that airports mitigates the risks and optimize resource allocation?
- Different sized airports: what is the difference from security cost and decision perspective?
- How does the risk perception of passengers and airport operators and social acceptance of security measures impact and can be modeled?
- New security measures and emerging threats, what is the balance between them in terms of cost and technology, security gain and risk perception of passengers?

These questions form the key requirements of this work package. Together with Work Packages 4, 5 and 6, by utilising the threats and the scenarios identified in the present report we aim to answer these questions above and build policy recommendations based upon those answers. Then through the engagement plan presented in Section 3 we aim to disseminate this information to airport security operators, decision makers and policy makers at the national and supranational level different levels in order to discuss and validate the results of WP1.

7. ANNEX – Airport Expenditures and Revenues

7.1 Airport operational expenditure

Security related operational expenditure includes those costs related to the provision of security activities by the airport, and reflected in the profit and loss account. All references to operational costs or expenditures we will refer to are for security related activities as opposed to operational costs or expenditures for the airport business as a whole.

Within this group of operational expenditures, most airports include costs related to the following categories:

- Labour
- Outsourcing
- Insurance
- Maintenance
- Depreciation

In terms of the breakdown of security related operational expenditure, airport direct labour and outsourcing contracts are the 2 major expenditure areas accounting on average for about 1/3 each one of security related operational expenditure since 2002 up to now. Outsourcing mainly comprises the provision of passenger, hand baggage and surveillance responsibilities by a third party (normally a private security firm). As such, labour related cost is the largest expenditure item in airport security accounting for around 60% (o average) of total security operational expenditure for European Airports.

Labour costs are followed by police costs, accounting for a further 15%. In several States, including Switzerland and the UK, police undertake certain key airport security activities such as terminal and airport surveillance. The airports generally cover the cost of providing these activities. Other minor security operational costs include insurance, maintenance and depreciation.

Indirect costs represent a further 8%-10%, of which company overheads is the largest item. Expenditure levels on background checks, IT and training are relatively small.

In general, airports have experienced large increases in security related expenditure after 11 septemeber 2001. These expenditures became almost constant in recent years.

Not surprisingly, the larger airports experienced the biggest absolute increases in security expenditure. However, the rise in security expenditure may well be proportionately more important for the medium and small European airports. This is due to not having large volumes of passengers to spread the impact of costs.

Some security related costs such as terminal and perimeter surveillance could be considered to be fixed costs (driven by an airport’s infrastructure rather than traffic throughputs). Other costs such as passenger, baggage and staff screening depend to a larger extent on the airport’s passenger and airfreight throughputs (hourly and seasonal distribution are also key factors) and therefore could be deemed as variable or semi-variable costs. Increased throughput is likely to require incremental expenditure on staff and equipment when any excess capacity is fully utilised.

Often increases in security related expenditure exceed throughput growth rates.

For example, in Amsterdam-Schiphol the expenditure increases were primarily a result of centralising passenger and hand baggage screening activities. Largely in the past and also still today depending on the destinations, screening is carried out at the departure gate with the change driven by the transfer of the screening responsibility from the State authority (i.e. Royal Port Police) to the airport in

April 2003. Schiphol also introduced 100% staff screening and biometric systems during the 2003-2005 period.

Many other airports, including medium and small sized airports, recorded a similar experience with increases in costs significantly outstripping increases in throughputs.

A number of other responding airports have experienced rising security expenditure in spite of either flat or reducing passenger throughputs.

Airport security capital investment

Capital expenditure investment in security related activities has risen sharply due to new security standards arising in the aftermath of 11 September 2001 as well as the mandated requirements and timescales in Regulation (EC) No 2320/2002 [3], particularly those related to screening of hold baggage, have required some airports to significantly increase investment in security related equipment and facilities.

Airports use to break their capital expenditure into 3 areas:

- Equipment: expenditure related to the acquisition and installation of new security equipment including hold baggage screening devices, explosive detection systems (EDS), x-ray machines, CCTV equipment, biometric readers, etc.
- Terminal redevelopment: expenditure on the modification or expansion of terminal facilities necessary to accommodate new security procedures and equipment e.g. baggage make-up areas, check-in halls, etc.
- Others: any other security related investment that cannot be categorised under the other 2 groups. For example, some airports have tightened access to restricted areas; others have strengthened perimeter fences, etc.

7.2 Security Revenues and Competition Issue

The airports under the decentralised model (where responsibility for key security activities rests with the airport operator or third party) appear to be at a disadvantage compared to airports under the centralised model (where the responsibility rests with the State). Airports under the decentralised model reported an average operating deficit of €1.22 per passenger, versus airports under the centralised model with an average deficit of €0.52.

Within both models there are variances between the States. The net airport position in some States produced a surplus whilst in others it resulted in a deficit. This also occurs for State revenues and costs with some States posting a surplus and others a deficit. However, for States, there is little difference with broadly matching operating results under both models.

Carriers that levy a specific security charge generated an average operating surplus of €0.30 per passenger. When those carriers that incurred costs but did not levy a security surcharge are included, a net deficit of €0.19 per passenger was reported. As with the States and airports, some carriers reported a surplus and others a deficit.

8. ANNEX – Additional Security Measures for Special Cases

Screening of passengers with reduced mobility

Passengers with reduced mobility shall be subject to screening in such a way as to ensure that no prohibited articles are on or about the person being screened. The search shall be carried out as fully as the nature of the disability allows it. If a wheelchair or stretcher is being used that too shall be searched.

Where available, it is recommended, that a wheelchair, which does not activate WTMDs, is used by persons with reduced mobility. This recommendation originates from ECAC Doc 30 [4] and relates to airports with more than 100,000 passengers per year. Additional guidelines are in Attachment VII to Annex IV-12-A of ECAC Doc 30.

Security provisions for potentially disruptive passengers

Specific security measures shall be introduced for the following groups of potentially disruptive passengers:

1. deportees;
2. inadmissible persons;
3. persons in lawful custody.

These specific security measures relate to notification to the air carrier and the pilot-in-command as well as additional requirements for screening.

In accordance with Decision 4333 the following supplementary safeguards for potentially disruptive passengers apply:

1. stringent screening of them and their cabin and hold baggage;
2. boarding prior to all other passengers, subject to coordination with the airline or pilot in command;
3. no occupancy of aisle seats or seats next to emergency exits;
4. no access to alcohol;
5. sufficient number of escorts, if deemed necessary in the risk assessment;
6. escorts shall be able to converse with the aircraft crew;
7. no public disclosure of the flight schedule for transporting potentially disruptive passengers; and
8. restraining devices shall be provided, if deemed necessary in the risk assessment.

More detailed guidance on potentially disruptive passengers is in Annex IV-4-D of ECAC Doc 30.

Specific security measures shall be introduced for unruly passengers. Unruly passengers are persons who commit on board a civil aircraft, from the moment when the aircraft door is closed prior to take-off to the moment when it is reopened after landing, an act of assault, intimidation, damage to an aircraft, etc. Guidance on the handling of unruly passengers is provided in Annex IV-4-C of ECAC Doc 30.

Screening of cabin baggage using high definition x-ray equipment with TIP installed.

Where cabin baggage is screened by high definition x-ray equipment that has TIP installed and employed then:

1. the screener shall be given no more than 30 seconds to respond to an image of a bag before, where applicable, a message is presented in accordance with rules defined in section;

2. where a message is presented indicating that a virtual image of a threat article was projected, the screener shall clear the message and then analyse the image of the bag again for prohibited articles.

A virtual image of a threat article shall, on a random basis, be projected within at least 1% and not more than 3% of images of bags.

Persons other than passengers

Screening of persons other than passengers and items carried as set out in Regulation 300/2008 [6] shall be the following:

1. Persons other than passengers, together with items carried, shall be screened before being allowed access into security restricted areas in order to prevent prohibited articles from being introduced into these areas; or
2. Where this is not practicable, then persons and items shall be subjected to continuous appropriate random screening at a frequency indicated by risk assessments conducted by the competent authority in each Member State;
3. All persons other than passengers, together with items carried, shall be screened upon entering critical parts of security restricted areas in order to prevent prohibited articles from being introduced into these parts. Critical parts of security restricted areas need to be defined at each airport. However, Regulation 1138/2004 states that staff need not be screened before being allowed access to critical parts of SRA if they are escorted by a screened and authorised staff member.

According to regulation No 300/2008 [6], States may apply more stringent measures than those defined by common standards in Article 4 of the Regulation. Therefore the procedures may vary between States.

Persons, including flight crew members, shall have successfully completed a background check before either a crew identification card or an airport identification card authorising unescorted access to security restricted areas is issued to them.

In addition to the regular checks of passengers and other persons, there shall be surveillance, patrols and other physical controls at airports, and where appropriate, in adjacent areas with public access, to identify suspicious behaviour of persons and to reveal any vulnerabilities which could be exploited to carry out an act of unlawful interference.

When screening persons other than passengers, security staff may refuse any member of staff in possession of an article over which they have concern access to a security restricted area.

Procedure for screening staff and items carried

Prohibited articles of category 1 to 5 may only be carried into the SRA or on board an aircraft by staff, including flight crew, if they are authorised to do so by the appropriate authority in order to undertake tasks that are essential to the operation of airport facilities or aircraft or for the performance of in-flight duties. These prohibited articles may be left in a security restricted area or on board an aircraft provided they are kept in secure conditions.

Prohibited articles of category 6 (see section 0) may be carried into the security restricted area or on board an aircraft by staff; including flight crew.

Prohibited articles of category 1 to 5 (see section 0) may be carried and left in a SRA or on board an aircraft provided they are kept in secure conditions.

Screening of hold baggage

Hold baggage can be classified as accompanied and unaccompanied.

The air carrier shall ensure that every passenger travels on the same flight as their checked hold baggage. Where this is not the case, that hold baggage shall be considered as unaccompanied baggage.

The following methods, either individually or in combination, shall be used to screen hold baggage:

1. a hand search; or
2. x-ray equipment; or
3. Explosive Detection Systems (EDS) equipment; or
4. Explosive Trace Detection (ETD) equipment.

Where the screener cannot determine whether or not the hold baggage contains any prohibited articles, it shall be rejected or rescreened to the screener's satisfaction.

A hand search shall consist of a thorough manual check of the baggage, including all its contents, so as to reasonably ensure that it does not contain prohibited articles.

Where x-ray or EDS equipment is used, any item whose density impairs the ability of the screener to analyse the contents of the baggage shall result in it being subject to another means of screening.

Screening by explosive trace detection (ETD) equipment shall consist of the analysis of samples taken from both the inside and the outside of the baggage and from its contents. The contents may also be subjected to a hand search.

As far as non-nominal operations (i.e. operations that take place not according to plan) are concerned, the appropriate authority shall set out in its national civil aviation security programme detailed procedures how the screening objective shall be met in case of screening equipment failure. Therefore procedures can vary between Member States.

Screening of hold baggage using EDS

Where an EDS is used and a piece of hold baggage generates an alarm, then the piece of hold baggage shall be screened again by:

1. a screener viewing the image of the bag produced by the EDS; or
2. a second EDS that both meets a higher standard than the first EDS used and is in automatic mode; or
3. a second EDS that is used in a manner that allows a more detailed examination of the bag by the screener; or
4. a hand search; or
5. conventional x-ray equipment, with each bag being viewed from two different angles by the same screener at the same screening point; or
6. trace detection equipment, whereby samples taken from both the inside and outside of the bag and from its contents shall be analysed.

Any item whose density impairs the ability of the equipment of the screener to analyse the contents of the hold baggage shall result in the bag being subject to another means of screening that is not subject to the same impairment.

Screening of accompanied hold baggage using conventional x-ray equipment with TIP installed and employed

Where accompanied hold baggage is screened by conventional x-ray equipment that has TIP installed and employed, the same procedures apply as for cabin baggage.

Protection of hold baggage

Passengers may not be allowed access to screened hold baggage, unless it is their own baggage and they are supervised to ensure that**Errore. L'origine riferimento non è stata trovata.**:

1. no prohibited articles as listed in Attachment 5-B of the Regulation 185/2010 [7] (ammunition, detonators, mines, etc.) are introduced into the hold baggage; or
2. no prohibited articles as listed in Attachment 4-C of the Regulation 185/2010 [7] (the same which is included in section 0) are removed from the hold baggage and introduced into the security restricted areas or on board an aircraft.

Hold baggage that has not been protected from unauthorised interference shall be rescreened.

Cargo, mail and other goods

Rules which apply to cargo and mail are as follows:

All cargo and mail shall be subjected to security controls prior to being loaded on an aircraft. An air carrier shall not accept cargo or mail for carriage on an aircraft unless it has applied such controls itself or their application has been confirmed and accounted for by a regulated agent, a known consignor or an account consignor.

1. Transfer cargo and transfer mail may be subjected to alternative security controls to be detailed in an implementing act.
2. Transit cargo and transit mail may be exempted from security controls if it remains on board the aircraft.

Cargo and mail shall be protected from unauthorised interference from the point at which security checks are applied.

Air carrier mail and air carrier materials shall be subjected to security controls and thereafter protected until loaded onto the aircraft in order to prevent prohibited articles from being introduced on board an aircraft.

A subject to security controls should also be these items (referred to as other goods):

1. air carrier mail and air carrier materials – these shall either be screened as hold baggage or subjected to the same security controls as for cargo and mail. Air carrier mail and air carrier materials to be loaded into any part of an aircraft other than the hold shall be screened as cabin baggage;
2. in-flight supplies, including catering, intended for carriage on board an aircraft - screening check, unless:
    a) security controls have been applied to the supplies by an air carrier that delivers these to its own aircraft and the supplies have been protected from unauthorised interference from the time that those controls were applied until delivery at the aircraft; or

b) security controls have been applied to the supplies by a regulated supplier and the supplies have been protected from unauthorised interference from the time that those controls were applied until delivery at the aircraft or, where applicable, to the air carrier or another regulated supplier; or

c) security controls have been applied to the supplies by a known supplier and the supplies have been protected from unauthorised interference from the time that those controls were applied until delivery to the air carrier or regulated supplier.

3. airport supplies, ie supplies intended to be sold or used in security restricted areas of airports, including supplies for duty-free shops and restaurants – screening check, unless security controls have been applied to the supplies by a known supplier and the supplies have been protected from unauthorised interference from the time that those controls were applied until they are in the security restricted area.

Part F of the Annex to the Regulation 272/2009 [9] defines the following conditions under which cargo and mail to be loaded on an aircraft shall be screened or subjected to other security controls:

1. security controls have been applied to the consignment by a regulated agent and the consignment has been protected from unauthorised interference from the time that those security controls were applied; or
2. security controls have been applied to the consignment by a known consignor and the consignment has been protected from unauthorised interference from the time that those security controls were applied; or
3. security controls have been applied to the consignment by an account consignor, the consignment has been protected from unauthorised interference from the time that those security controls were applied, and the cargo is carried on an all-cargo aircraft or the mail on an all-mail aircraft; or
4. security controls have been applied to transfer cargo and transfer mail, as referred to in point 6.1.2 of the Annex to Regulation (EC) No 300/2008 [6] - this point says that transfer cargo and transfer mail can be subject to alternative security controls.

Cargo, courier and express parcels can be delivered to airport by regulated agent, known consignor or even an entity which is not a regulated agent. However, such entity has to comply with the same security requirements as regulated agent. These requirements are described in detail in section 6.

As far as mail is concerned, letters which are below a specified weight and dimension may be exempted from security controls. The maximum weight and dimension for such letters shall be 250 grams and thickness 6mm thickness.

Security procedures for supplies of liquids and tamper-evident bags.

"Checks" shall be made on supplies of liquids and supplies of tamper-evident bags, unless a known supplier (see definition) applies security controls. Checks is a visual check by authorised staff for signs of interference, in particular tampering with seals, theft and the introduction of prohibited articles.

9. ANNEX – IATA Security Trainings

The International Air transport Association (IATA) offers the following security courses:

- Predictive passenger screening;
- Airport security operations;
- Basic AVSEC management course for airport and airline operators;
- Management of aviation security;
- Security management systems for airports and civil aviation authorities (SEMS);
- Security quality control;
- Security risk and crisis management;
- Senior management of aviation security; and
- Cargo security.

Predictive Passenger Screening

The objectives of the course are to:

- identify, anticipate security and terror threats;
- assess a passenger's level risk using a variety of information obtaining tools;
- create a culture of awareness within your organization;
- evaluate passenger data during the security check processes; and
- apply questioning techniques to obtain additional information from passenger.

The course was designed for:

- security managers;
- security screening supervisors; and
- screening security personnel.

The outline of the course is as follows:

- security threats and terrorism (including threats to civil aviation, current terror threats and modus operandi of terror groups);
- screening technologies (including traditional security screening implementation, behavior analysis system, and concealment techniques);
- detecting suspicious signs (reading body language, observation techniques);
- evaluating travel documents (including passenger data (PNR/PNI) and travel documents as indicators);
- questioning techniques (including collecting information from passengers); and

Airport Security Operations

The objectives of the course are to:

- find out about the updated International Standards and Recommended Practices (SARPs);
- learn to plan and implement airport security measures;
- develop and improve your emergency response plans;
- evaluate airport security threats; and
- get updated information from industry experts on the latest systems and procedures.

The course was designed for:

- airport/airline security managers and officers;
- law enforcement personnel involved in airport operations;

- managers from companies involved in airport operations; and
- government representatives involved in Security, Customs and Immigration.

The outline of the course is as follows:

- global civil aviation security structure;
- threats & risks to civil aviation;
- security legislation;
- Annex 17 [3] & Security Manual;
- access control;
- inspections of passengers & baggage;
- technology & equipment in security;
- counter-sabotage measures;
- security and passenger facilitation;
- contingency planning; and
- response to security emergencies.

Basic Avsec Management Course For Airport And Airline Operators

The objectives of the course are to:

- provide a comprehensive and practical understanding of the essential foundations of aviation security;
- offer the experience of certified instructors from both IATA and AVSECO;
- relate to the aviation security responsibilities and requirements of both airline and airport operators;
- present the essential technical and managerial skills; and
- incorporate the legal basis of and legal requirements arising from a national aviation security programme.

The course was designed for:

- airport managerial staff wishing to refresh their knowledge in aviation security and management skills;
- airline security managers and security advisors;
- management level staff of airline shipping agents and air cargo handlers;
- law enforcement agency officers whose work relates to aviation, or other mass transport related operations;
- professionals interested in furthering their professional knowledge and managerial skills relating to aviation security; and
- new staff managing aviation security functions as service provider, regulator or end user.

The outline of the course is as follows:

- threat to Civil Aviation;
- IATA’s role in AVSEC & Security Manual;
- ICAO’s role in AVSEC & Annex 17 [3];
- hold baggage screening system;
- baggage reconciliation;
- airport access control system;
- HKIA permit system;
- Security Management Systems;
- crisis management;
- risk management;

- in-flight security;
- role of flight attendants;
- cargo security and regulated agent regime;
- facilitation and security;
- technology & equipment;
- zero tolerance; and
- case studies.

Management Of Aviation Security

This course should allow participants to build a safe and secured global air transportation system through the implementation of enhanced regulations, reliable technology and best management practices.

The objectives of this training course are to:

- acquire knowledge, technique and skill in developing and managing international civil aviation security, as well as in measuring its performance;
- target resources appropriately and measuring results;
- identify and manage security-risks;
- communicate effectively on security with the Civil Aviation Authority, airlines, cargo agencies, airport service providers and other security agencies;
- build a security culture in the aviation environment;
- manage organizations and instill a systemic approach to aviation security;
- integrate human factors to the civil aviation security system;
- evaluate the operation of the security system;
- ensure continued compliance with aviation security standards;
- prepare organisations for audit by external bodies;
- move aviation security measures towards full integration with all airport and airline process;
- ensure that security measures add value to the airport and airline; and
- move towards a secure passenger and cargo experience.

The course was designed for:

- representatives from civil aviation authorities;
- experienced managers from airline operators, airport operators and airport service providers including those involved with either passenger and/or cargo operations;
- experienced airline and airport security managers and supervisors;
- members of aviation-related boards of directors;
- appropriate authorities for aviation security;
- police authorities;
- narcotics control authorities;
- border control authorities; and
- armed forces representatives involved in airport security operations.

The course content is the following:

- the threat to civil aviation - past, present, and future;
- international and national security legislation;
- security programmes, Annex 17 [3] & Manual;
- access control;
- control of passengers and baggage;

- security of cargo, catering & stores;
- security programme adjustments;
- contingency planning;
- response to major security emergencies;
- threat assessment and risk management;
- job analysis, job description and recruitment;
- staff motivation: deployment, briefing & supervision;
- staff performance assessment;
- technology and equipment;
- quality control;
- security and facilitation: IATA security management systems; and
- civil aviation security management responsibilities.

The duration of the course is five days.

Security Management Systems For Airports And Civil Aviation Authorities (Sems)

The main objectives of the course are to:

- understand aviation security regulations in light of changing needs of global civil aviation;
- learn to take a more pro-active and layered approach to security;
- identify the enhanced roles and responsibilities of security managers in the organization;
- establish a security department that fulfils all the corporate and operational needs;
- understand the need for applicable security measures and how to develop them;
- develop security measures that meet basic requirements and are recommended as ‘best practice’; and
- find the balance between efficient security and cost effectiveness.

The course was designed for:

- managers responsible for implementing security policy and procedures;
- security quality assurance managers; and
- senior and middle aviation security managers.

The course content is as follows:

- establishing a security organisation;
- fundamentals of human factors;
- threat assessment;
- integrated risk management;
- quality control;
- security audit and quality assurance;
- contingency planning;
- security systems design and implementation;
- change management strategies; and
- performance based regulations and requirements.

Security Quality Control

The objectives of the course are to:

- understand the standard operating procedures for aviation security audits;
- become familiar with the ICAO Annex 17 [3] requirements;

- increase awareness of international conventions;
- learn how to continuously update the aviation security program; and
- ensure compliance with aviation security requirements.

The course was designed for:

- airport and airline security managers and officers;
- security coordinators;
- law enforcement personnel involved in airport operations;
- managers from companies involved in airport operations; and
- government representatives involved in security.

The course content is the following:

- the role of ICAO in aviation security;
- audit of the national AVSEC program;
- Annex 17 [3] and the Security Manual;
- threat assessment;
- audit of airport security facilities;
- passenger terminal security measures;
- human factors;
- airline security;
- cargo security;
- security equipment; and
- training & employee awareness.

Security Risk And Crisis Management

The objectives of the course are to:

- learn how to stay ahead of emerging threats rather than reacting to them;
- understand the importance of employing effective information and intelligence;
- understand quantitative and qualitative risk analysis;
- understand risk management applied in ISO international standards;
- gain knowledge on effective deployment of current technology;
- master how to strategically evaluate countermeasures;
- understand the importance of planning for crises and potential dangers;
- learn how to involve stakeholders in the event of a crisis; and
- learn the elements of crisis management plans.

The course was designed for:

- airline managers of safety and security;
- airport managers of safety and security;
- civil aviation managers and directors;
- law enforcement officers responsible for aviation security; and
- security risk and compliance officers.

The course content is the following:

- threats and risks affecting aviation security;
- attacks on civil aviation: an historical perspective;
- risk analysis and risk management;
- areas of vulnerability, assessments and prioritising;
- building and facility security design and audit;
- strategic evaluation of security measures;
- technology integration;

- precipitators of an aviation security crisis; and
- stakeholders in aviation security.

Senior Management Of Aviation Security

This training package is focused on broadening of knowledge of a safe and secure global air transportation system, crisis management and worldwide best practices for senior managers.

The objectives of the course are to:

- develop senior management skills relating to international civil aviation security;
- examine current issues facing senior AVSEC management across various countries and jurisdictions;
- work towards reduction of the costs of implementing AVSEC measures;
- understand the concepts of asset protection, risk management and threat assessment;
- establish a means of effective communication with aviation security stakeholders;
- understand best practices throughout the aviation industry relating to security;
- examine practices relating to contract award, supervision and management;
- work towards maintaining a security culture in the aviation environment;
- manage the relevant organization with a systemic approach to aviation security;
- adopt concepts leading to greater customer satisfaction; and
- manage and evaluate all human factors in the civil aviation security system.

The course was designed for:

- representatives from civil aviation authorities;
- experienced managers from air operators, airport operators, and airport service providers including passenger and cargo interface;
- airline security management personnel;
- members of aviation boards of directors;
- representatives from the appropriate authorities for aviation security;
- police authorities;
- narcotics control agencies;
- border control and customs agencies;
- armed forces representatives involved in airport security operations;
- aviation security contract management; and
- flight and cabin crew management.

The course content is the following:

- introduction to senior management of AVSEC course;
- the threat to civil aviation – past, present and future;
- role of ICAO in AVSEC;
- issues and challenges facing senior AVSEC management;
- in-house security and outsourced security;
- AVSEC contract award, management and service level agreements;
- national AVSEC programmes;
- airport security programmes;
- air carrier security programmes;

- ground security measures;
- passenger terminal security measures;
- passenger baggage security measures;
- security for air cargo, catering and stores;
- security equipment technology;
- contingency planning and bomb threat management;
- quality control, audits, inspections and tests;
- management systems for the future; and
- aviation security as a source of industry added value.

Cargo Security

The objectives of the course are to:

- gain in-depth knowledge of the latest security initiatives, their implementation and implications;
- review selected government programs relating to air cargo security;
- plan and execute effective crisis management strategies;
- minimise your operational exposure through proper risk management techniques;
- benefit from "hands-on" learning with industry leaders; and
- review and discuss Annex 17 [3] recommendations and guidelines.

The course was designed for:

- cargo services and operational managers;
- cargo acceptance and handling staff;
- customs officers;
- security managers;
- risk management specialists;
- aviation and AVSEC inspectors; and
- terminal and airport managers.

The course content is the following:

- the threat to civil aviation;
- regulatory authorities;
- principles of air cargo security;
- cargo security acceptance;
- exemptions to screening;
- recognition and handling of improvised explosive devices;
- x-ray screening;
- cargo terminal access control;
- employee security awareness;
- cargo security training;
- cargo security auditing; and
- handling a bomb threat.

REFERENCES

[1] Civil Aviation Security Financing Study, Irish Aviation Authority and Avia Solutions, 2004.
[2] International Security and Development Cooperation Act, 99th Congress of USA, 1985.
[3] ICAO, Annex 17, Security Safeguarding International Civil Aviation Against Acts of Unlawful Interference, Chicago, 2011.
[4] ECAC Doc 30 – ECAC Policy Statement in the Field of Civil Aviation Security, 12th Edition, July 2003.
[5] EC Regulation No 2320/2002, European Commission, 2002.
[6] EC Regulation No.300/2008, European Commission, 2008.
[7] EC Regulation No. 185/2010, European Commission, 2010.
[8] EC Regulation No 820/2008, European Commission, 2008.
[9] EC Regulation No 272/2009, European Commission, 2009.
[10] EC Decision 4333/2008 laying down additional measures for the implementation of the common basic standards on aviation security, European Commission, 2008.
[11] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
[12] ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls
[13] NIST Special Publication 800-53 Revision 3 - Recommended Security Controls for Federal Information Systems and Organizations
[14] Shim, W., Massacci, F., de Gramatica, M., Tedeschi, A., Pollini, A. (2013) Evaluation of Airport Security Training Programs: Perspectives and Issues. SecATM 2013: International Workshop on Security in Air Traffic Management and other Critical Infrastructures. ARES 2013. Regensburg, Germany.
[15] Cornish, D. B., Clarke, R. V. (2011) The Reasoning Criminal: Rational Choice Perspectives on Offending (Research in Criminology). Springer, London, 1986. Reprint 2011.
[16] Shim, W., Allodi, L., Massacci, F. (2012) Crime Pays If You Are Just an Average Hacker, Cybersecurity, pp.62-68, 2012 International Conference on Cyber Security, 2012
[17] Cornish, D. B., Clarke, R. V. (1987) “Understanding crime displacement: An application of
rational choice theory. Criminology, 25(4):933{948,1987.
[18] Group IB. (2011) State and trends of the russian digital crime market. Technical report, Group IB, 2011.
[19] Motoyama, M., McCoy, D., Savage, S., Voelker, G.M. (2011) An analysis of underground forums. In Proceedings of the ACM 2011 Internet Measurement Conference, 2011.
[20] Taylor, P.A. (1999) Hackers: crime in the digital sublime. Psychology Press, 1999.
[21] Turgeman-Goldschmidt, O. (2005) Hackers' accounts: Hacking as a social entertainment. Social Science Computer Review, 23(1):8, 2005.
[22] Gerstein, D. (2009) Bioterror in the 21st Century: Emerging Threats in a New Global Environment. Annapolis, MD: Naval Institute Press, 2009. 256 pp., $25.95 paperback. ISBN: 978-1-59114-3.
[23] Borum, R. (2010). Understanding terrorist psychology. In Andrew Silke (Ed.) The Psychology of Counter-terrorism Oxon, UK: Routledge. ISBN: 978-0-415-55840-2