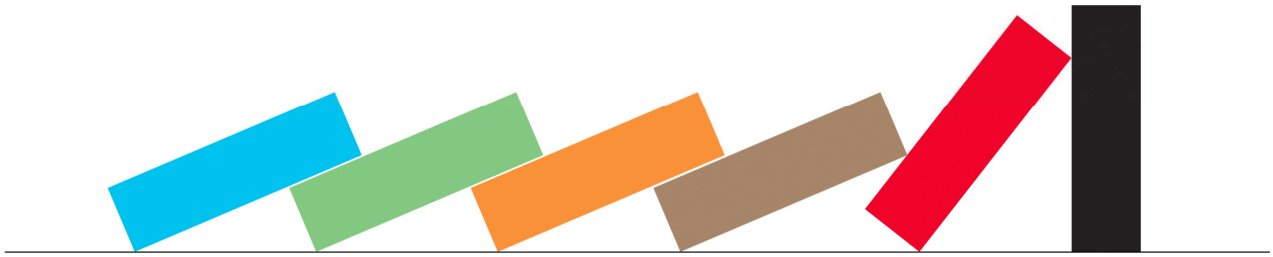

SECONOMICS

D1.2 – Airport Requirements first version

V. Meduri, F. Quintavalli, A. Tedeschi (DBL), B. Açikel, N. Ergün, U. Turhan(AU), M. De Gramatica, Woohyun Shim (UNITN), D. Rios Insua (URJC), J. Williams (ABDN)

Document Number	D1.2
Document Title	Airport Requirements first version
Version	0.8
Status	Final
Work Package	WP 1
Deliverable Type	Report
Contractual Date of Delivery	31.07.2012
Actual Date of Delivery	03.08.2012
Responsible Unit	DBL
Contributors	AU, UNITN, ABDN, SNOK
Keyword List	Airport Security, Regulators, Scenarios.
Dissemination level	PU

SECONOMICS Consortium

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

1	UNIVERSITÀ DEGLI STUDI DI TRENTO	Università Degli Studi di Trento (UNITN) 38100 Trento, Italy www.unitn.it	Project Manager: prof. Fabio MASSACCI Fabio.Massacci@unitn.it
2	DEEPBLUE	DEEP BLUE Srl (DBL) 00193 Roma, Italy www.dblue.it	Contact: Alessandra TEDESSCHI Alessandra.tedeschi@dblue.it
3	Fraunhofer ISST	Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., Hansastr. 27c, 80686 Munich, Germany http://www.fraunhofer.de/	Contact: Prof. Jan Jürjens jan.juerjens@isst.fraunhofer.de
4	Universidad Rey Juan Carlos	UNIVERSIDAD REY JUAN CARLOS, Calle TulipanS/N, 28933, Mostoles (Madrid), Spain	Contact: Prof. David Rios Insua david.rios@urjc.es
5	UNIVERSITY OF ABERDEEN	THE UNIVERSITY COURT OF THE UNIVERSITY OF ABERDEEN, a Scottish charity (No. SC013683) whose principal administrative office is at King's College Regent Walk, AB24 3FX, Aberdeen, United Kingdom http://www.abdn.ac.uk/	Contact: Prof. Julian Williams julian.williams@abdn.ac.uk
6	TMB Transports Metropolitans de Barcelona	FERROCARRIL METROPOLITA DE BARCELONA SA, Carrer 60 Zona Franca, 21-23, 08040, Barcelona, Spain http://www.tmb.cat/ca/home	Contact: Michael Pellot mpellot@tmb.cat
7	Atos	ATOS ORIGIN SOCIEDAD ANONIMA ESPANOLA, Calle Albarracin, 25, 28037, Madrid, Spain http://es.atos.net/es-es/	Contact: Silvia Castellvi Catala silvia.castellvi@atosresearch.eu
8	SECURENOK	SECURE-NOK AS, Professor Olav Hanssensvei, 7A, 4021, Stavanger , Norway Postadress: P.O. Box 8034, 4068, Stavanger, Norway http://www.securenok.com/	Contact: Siv Houmb sivhoumb@securenok.com
9	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	02/05/2012	Draft	A . Tedeschi (DBL)	1st Draft
0.2	15/06/2012	Draft	B. Açikel, N. Ergün, U. Turhan (AU)	AU Scenarios Provision
0.3	03/07/2012	Draft	V. Meduri, F. Quintavalli (DBL)	DBL Scenarios review and security requirement definition
0.4	18/07/2012	Draft	F. Quintavalli, A. Tedeschi (DBL)	Document finalisation for internal review by UTN, ABDN and URJC
0.5	28/07/2012	Draft	F. Quintavalli, A. Tedeschi (DBL), B. Açikel, N. Ergün, U. Turhan (AU), M. De Gramatica, Woohyun Shim (UNITN), D. Rios Insua (URJC), J. Williams (ABDN)	ABDN commments addressed and final review before Quality Check
0.6	31/07/2012	Draft	E.Chiarani (UNITN)	Quality Check completed. Minor changes requested
0.7	01/08/2012	Final	F. Quintavalli, A. Tedeschi (DBL)	Changes fixed. Final version ready for submission
0.8	02/08/2012	Final	F. Massacci (UNITN)	Final check by the Coordinator before submission

INDEX

Executive summary

This deliverable will preliminarily identify and analyse the main issues for airport security by listing all the stakeholders and their mutual interactions, the security high-level requirements complemented by a preliminary set of narrative scenarios. The presented scenarios are quite general and of broad interest for Airport stakeholders and Aviation Authorities. They can be replicated, customised and assessed for all airports depending on their scale and structure. Airport security requirements will be detailed and formalized in D1.3, as well as a final set of narrative security-relevant scenario to which apply the models and tools provided by technical workpackages.

1. Introduction

1.1. Scope of the report

This report will identify and analyse the main issues for airport security. A range of techniques will be used, from interviews of key stakeholders, ethnographic observation, and collection of quantitative indicators whenever possible. Some of the key issues that will be addressed in this deliverable are:

- map all the relevant stakeholders and their different points of view,
- map all the interactions among the various groups of stakeholders,
- analyse the interactions between the airport and the travelling public.

The outcome will be a report describing the airport environment, listing all the stakeholders and their mutual interactions. And their regulatory minimal requirements (with explicit references and links to current European legislation) complemented by narrative scenarios.

The basic airport security requirements are applied by ICAO member states around the world. Additionally, member states are advised by ICAO that they can take extra security regulations and implementations depending on their structure and airport regions. All member states should facilitate national civil aviation security program. In this context, the scenarios which are presented can be assessed for all airports depending on their scale and structure. Unlawful interferences related ATM, airside and terminal can be generalised to the other airports. The weak points can be found in all airports to perform these interferences. For instance ATM related scenarios can be disastrous for the airports and airspaces which have heavy traffic load. Airport border interference can be performed for all developing airports since they are very close to the public areas. On the other hand the impacts can be generalised for all airport users and stakeholders.

The security requirements will be detailed and formalized in D1.3, as well as a final set of further detailed narrative security-relevant scenario to which apply the models and tools provided by technical workpackages. A preliminary analysis of models and tools for advanced risk assessment in the Airport Case Study will be presented and briefly discussed.

1.2. Project Objectives and Expected Results

The main objective of SECONOMICS is to develop innovative risk assessment 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 the formers and the latters 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 the Policy Makers face security issues, which interact with technical and socio-economic problems within a complex context.

1.3. Role of Case Studies in SECONOMICS

Using Case Studies in a research project is fundamental in order to understand which the real needs are, in this case in terms of security. Research can be abstract, Case Studies help researchers to follow a “realistic” path, from problem statement and definition of proper solutions to their implementation as “proof of concept”. The three different Case Studies are taken in order to describe in the best possible way how security issues affect the real world, in this case the transportation one. The Case Studies can be used and will be used also to validate the result of the research and to define the business models and market exploitation of SECONOMICS tools, guidelines and other outputs.

2. The Airport Case Study

Airport security refers to the techniques and methods used in protecting passengers, staff and aircraft which use the airports, from accidental/malicious harm, crime and other threats.
Large numbers of people pass through airports every day, this presents potential targets for terrorism and other forms of crime because of the high density of people co-located in a particular area.
Similarly, the potential high death rate due to attacks on aircraft and the ability to use a hijacked airplane as a lethal weapon may provide an alluring target for terrorism, whether or not they succeed, due their high profile nature following the various attacks and attempts around the globe in recent years.

Federal Aviation Administration defines main objectives of Aviation Security:
"The goal of aviation security is to prevent harm to aircraft, passengers, and crew, as well as support national security and counter-terrorism policy."

Airport security serves several purposes: to protect the airport facilities and aircraft from any threatening events, to reassure the traveling public that they are safe and to protect the country from external attacks

2.1. Airport Environment Description

A defined area on land or water (including any buildings, installations, and equipment) intended to be used either wholly or in part for the arrival, departure and surface movement of aircraft (ICAO, Annex 14).

Airport or airfield, place for landing and departure of aircraft, usually with facilities for housing and maintaining planes and for receiving and discharging passengers and cargo (Columbia Encyclopaedia, 2010).

As it's possible to understand from these two statements, the airport is a point of transfer and transport for people and goods between land and air; moreover, it is a social and shopping environment collecting people from public, business, aviation and security.
The airport is also the focal point of the Air Traffic Control (ATC) organisation: in fact, the sky has well defined structure and the ICAO defines it as a service provided in order to:

1 Prevent collisions between aircrafts and on the manoeuvring area between aircraft, vehicle and obstructions;
2 Expedite and maintain an orderly flow of air traffic.

Recently, a higher level of structure has been defined, called Air traffic Management (ATM), which is the aggregation of the airborne functions and ground-based functions (air traffic services, airspace management and air traffic flow management) required to ensure the safe\and efficient movement of aircraft during all phases of operations.

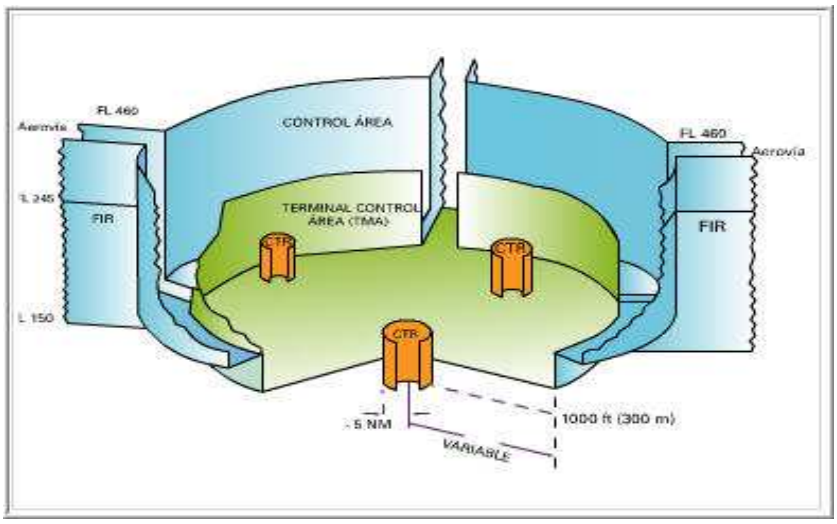

Figure 1 - Airspace Organisation.

Figure 1 is an example of the sky organisation from the ATC point of view:

- the blue zone is the Control Area (CTA), which is a space large enough to contain airways, or part of them, in order to provide ATC service to aircrafts; it is controlled by the ACC (Area Control Centre), the unit established to provide ATC service to controlled flights in CTAs under its jurisdiction.
- The green zone is the TMA/CTR (Terminal Control Area): when a CTA has heavy density of traffic and it is closed to a big airport, it is called TMA, and it is controlled by the TMA/APP (Terminal/Approach), the unit responsible for arriving and departing controlled flights.
- The orange zone is the ATZ (Aerodrome Traffic Zone), which is an airspace of defined dimensions established around an aerodrome for the protection of its traffic; it is controlled by TWR (Control Tower), which is the ATC unit established to provide ATC service to aerodrome traffic (ICAO Doc. 4444) that authorises the movement of any person, vehicle or aircraft inside the airport to prevent collisions. TWR area of responsibility is the Manoeuvring Area and the airspace around the airport, within a 5 miles radius, up to around a 3000 feet altitude. TWR has a central position to observe and manage all flights and depended operations on and around airport. Generally it becomes first contact point for all emergencies and urgencies in the airports.

So, as mentioned above, the Tower is a building situated inside the airport area, which is defined by ICAO too: it is divided in three areas, the **airside**, **landside** and **technical side**:

- The airside of an airport includes all the facilities that are associated with aircraft arrivals and departures including the control tower and all areas accessible to aircraft, including runways, taxiways and ramps.
- The airport landside is defined as the area bounded by the points at which passengers and goods enter the airport by all modes and the point on the apron at which the aircraft is serviced and loaded. The airport landside includes access roads, parking facilities, terminal facilities, and the aircraft apron.

- The technical side encompassed those functions that crossed over the air and land side boundaries, related primarily to the basic infrastructure and its upkeep. In some cases, IT infrastructure fell under this rubric.

Inside the landside there is the terminal, which is the area where passengers transfer between ground transportation and the facilities that allow them to board and disembark from aircraft.
Within the terminal, passengers purchase tickets, transfer and collect their luggage, go through security and wait for departure.
The buildings that provide access to the airplanes (via gates) are typically called **concourses**.

- *Pre - Security*
  - Check-in Counters
  - Retail stores and restaurants
- *Post - Security*
  - Duty-free Shops
  - Retail stores and restaurants
  - Airport Lounges
  - Airport Customs
  - Baggage Claim

2.2. Airport Stakeholders

The *airport* is a complex environment and this degree of complexity leads to consider it even as a whole entity, like every city could be. The different stakeholders working inside the airport can be considered as the organisations which hold the responsibility for the several activities which take place inside and outside the airport.
It is possible to state that airports can be considered as open systems, thinking that it is hard to trace clear boundary around them, as they are usually connected in multiple ways to the surrounding space (road, railways, etc.) and infrastructures (shopping and business centres, hotels, neighbour villages, university campus, etc.).
In addition to this, airports affect and are affected both internally and externally: external infrastructures, as the ones mentioned above in brackets, have a strong influence on the airport life. It is easy to imagine how a traffic jam in the highway from the city centre to the airport can lead to delays for passengers arriving at the airport, with consequent delays at the check-in or security checks. On the internal side, airport can be defined as a tightly coupled system: crisis events, that may affect one part of an airport, will likely have consequences on all others parts of the airport organization; as an example, a breach of security in the handling department, for example, will have a domino effect on control tower decisions concerning delaying and rerouting aircraft, which in turn affects the flow of passengers.
It is relevant to remember that inside the airport there are two kind of infrastructures: the logical one, which include the IT systems (i.e. Tower control systems), and physical side, as buildings, aircraft or check-in stations.
This complexity represents a disadvantage for the airport, especially from the security point of view: breaches can be easily found if the security issue is not taking seriously into account from all the different stakeholders.

Hereafter, it is possible to find two Tables, Table 1 and Table 2 with a list of stakeholders, working inside the airport organisation, divided for landside and airside.

LANDSIDE

Table 1 - Landside Stakeholders.

Stakeholder	Typology	Main mission in airside operations
Passengers	Departing, arriving, transferring	Sitting in the aircraft waiting for take-off or for disembark (after landing)
Airport Operators	Private companies, National CAA	Provides the solutions for passengers/goods movements to the airplane (on the aprons).
ANSP	Public and private companies, Military	TWR is responsible for aircraft manoeuvre, except for the apron, and for people/vehicle movements
Airspace Users	Passengers and goods	Landing, Taxi, Parking, Push-back/Towing, Taxi, Take-off
Public Services	Public and Private companies	Ensure public safety and health, addressing different emergencies

It is easy to understand that most of the stakeholders work both on the landside and the airside, with different tasks, but their final aim is to assist, as well as possible, the very final user of the airspace, the passengers.

AIRSIDE

Table 2 -Airside Stakeholders.

Stakeholder	Typology	Main mission in landside operations
Passengers	Private	Use airports to embark onto and disembark from aircraft
ANSP	Public and Private companies, Military	Air Traffic Management (ATM) information to airport operators
Airport Operators	Private companies, National CAA	Manage airport operations, sell space to retail outlets and airlines, parking, manage security, etc.
Airspace Users	Passengers and goods	Allow passengers to access aircraft, load and unload goods from cargo, sell tickets, and other passengers and goods assistance (e.g. lost baggage or

		special needs)
Handlers	Private companies	Manage the passengers, baggage and goods flow from check-in to aircraft and from aircraft to baggage reclaim
Security Operators	Private/ Public	Manage security of airport (e.g. access to restricted areas), flight security and passenger identification
Public Services	Public	Ensure public safety and health, addressing different issues

While some countries may have an agency that protects all of their airports (such as Australia, where the Australian Federal Police responsible for security at their major airports), in other countries like the United States, the protection is controlled at the state or local level. The primary personnel will vary and can include:

- A police force hired and dedicated to the airport i.e. the Irish Airport Police Service
- A branch (substation) of the local police department stationed at the airport
- Members of the local police department assigned to the airport as their normal patrol area
- Members of a country's military
- Members of a country's airport protection service
- Police dog services for explosive detection, drug detection and other purposes

Other resources may include:

- Security guards
- Paramilitary forces
- Military forces

2.3. Airport Security Procedures

Security should be an interest and somehow a mission that every stakeholder should carry on. On the other side, it seems that every country understands this issue, considering it sometimes as a real business. The general perception, by the way, is that the level of security is worldwide high, with rather high peaks, such as US or Israel.
Some incidents have been the result of travellers being permitted to carry either weapons or items that could be used as weapons on board aircraft so that they could hijack the plane. Travellers are screened by metal detectors. Explosive detection machines used include X-ray machines and explosives trace-detection portal machines (a.k.a. "puffer machines"). In the United States, the Transportation Security Administration (TSA) is working on new scanning machines that are still effective searching for objects that aren't allowed in the airplanes but that don't depict the passengers in a state of undress that some find embarrassing. Explosive detection machines can also be used for both carry on and checked baggage. These detect volatile compounds given off from explosives using gas chromatography.

A recent development is the controversial use of backscatter X-rays to detect hidden weapons and explosives on passengers. These devices, which use Compton scattering, require that the passenger stand close to a flat panel and produce a high resolution image A technology released in Israel in early 2008 allows passengers to pass through metal detectors without removing their shoes, a process required as walk-though gate detectors are not reliable in detecting metal in shoes or on the lower body extremities. Alternately, the passengers step fully shod onto a device which scans in under 1.2 seconds for objects as small as a razor blade. In some countries, specially trained individuals may engage passengers in a conversation to detect threats rather than solely relying on equipment to find threats.

Generally people are screened through airport security into areas where the exit gates to the aircraft are located. These areas are often called "secure", "sterile" and airside. Passengers are discharged from airliners into the sterile area so that they usually will not have to be re-screened if disembarking from a domestic flight; however they are still subject to search at any time. Airport food outlets have started using plastic glasses and utensils as opposed to glasses made out of glass and utensils made out of metal to reduce the usefulness of such items as weapons.

In the United States non-passengers were once allowed on the concourses to meet arriving friends or relatives at their gates, but this is now greatly restricted. Non-passengers must obtain a gate pass to enter the secure area of the airport. The most common reasons that a non-passenger may obtain a gate pass is to assist children and the elderly as well as for attending business meetings that take place in the secure area of the airport. In the United States, at least 24 hour notice is generally required for those planning to attend a business meeting inside the secure area of the airport. Other countries, such as Australia, do not restrict non-travellers from accessing the airside area, however non-travellers are typically subject to the same security scans as travellers.

Sensitive areas in airports, including airport ramps and operational spaces, are restricted from the general public. Called a SIDA (Security Identification Display Area), these spaces require special qualifications to enter.

2.4.

3. Airport Security Scenarios

Scenarios will be used to define research criteria and to write and define the models, and afterwards, to validate them.
This chapter describes how they have been identified, for both high-level scenarios that reflect the application modality, improvement and/or introduction of a security measure in the current legislation and the low level ones, which describe the local implementation of a security measure to avoid threats and malicious attacks. The mutual relationships among high-level and local operational scenarios are summarized in Figure 2.
A brief description of each scenario, the involved actors, the security issue and its socio-economic impact is given.

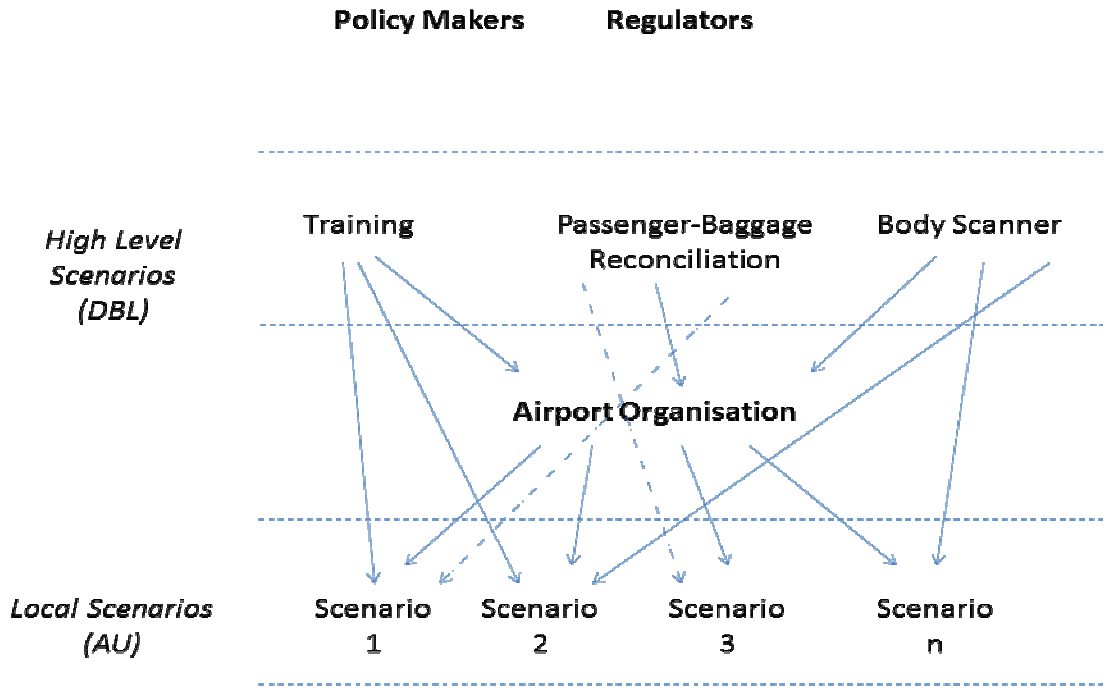

Figure 2 - High-level and Operational Scenarios in the Airport Case Study.

3.1. The 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 divide the scenarios in high level and low level ones: first ones represent general aspects of airport security, that are under discussion worldwide by institutional stakeholders. Second ones affect local decisions to effectively implement the single security measure. Experts of airport domain are Deep Blue and Anadolu University.
Figure 3 shows the interactions among Case Studies and technical workpackages.

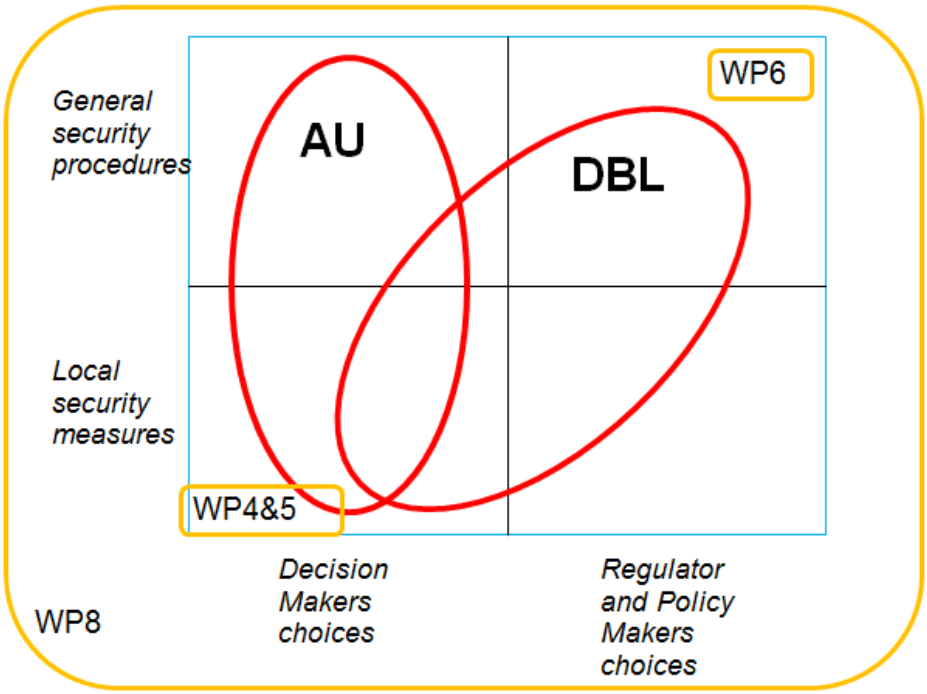

Figure 3 - Collaboration with Technical Workpackages in the Airport Case Study.

As it is possible to recognise from the sketch above, AU and DBL are responsible to create the two level scenarios, which are addressed to two different targets: the low-level one will interest decision makers of the airport, so it is possible to be defined as local; the high-level one, instead, will be interest of Regulator and Policy Makers (National CAAs and other organisation). Figure 4 introduces the scenarios: DBL will work on Passenger-Baggage Reconciliation, Body Scanner introduction and Training of Airport Personnel; AU will work on Unlawful Access to the Tower, Unlawful Interference with Apron, Unlawful Interference with Airside and Unlawful Interference with Security Checks.

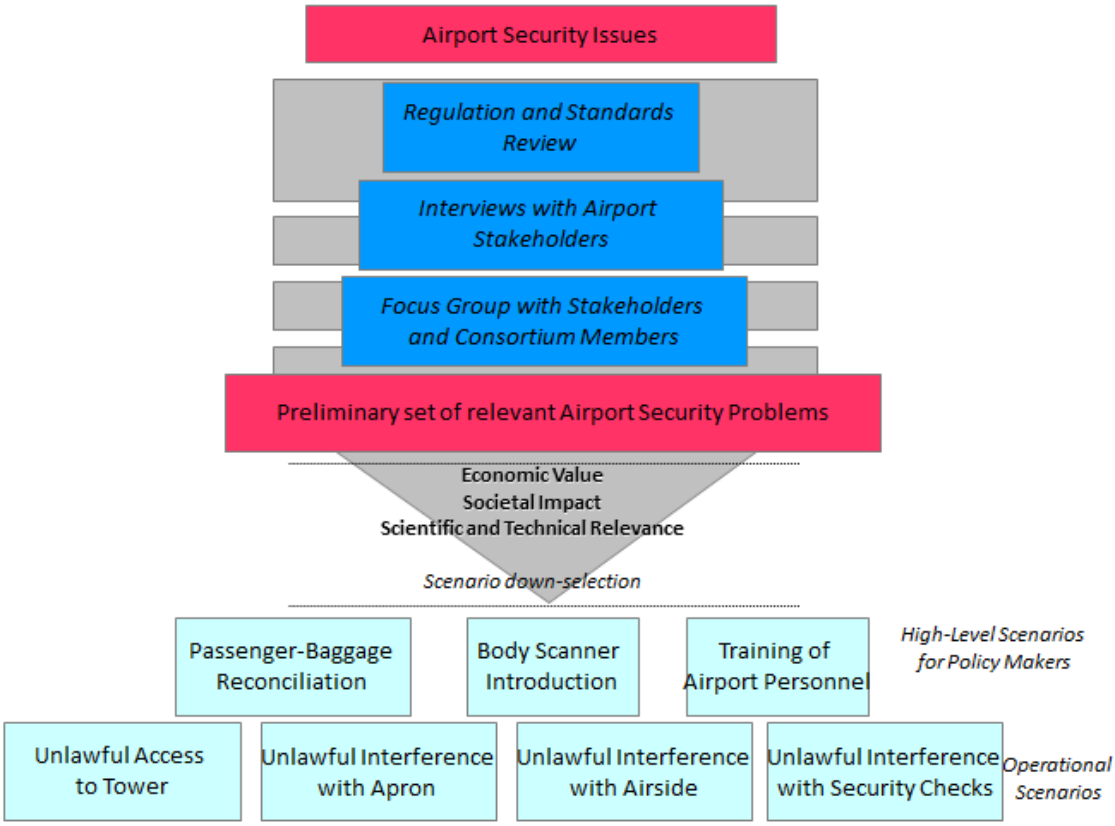

Figure 4 - Scenario Selection Process in the Airport Case Study.

3.2. High Level Airport Security Scenarios for Policy-Makers

A preliminary set of Security narrative scenarios have been collected during interviews with Airport Security stakeholders carried out by Deep Blue during the period April – June 2012.
The identified scenarios have been refined and detailed during the first WP1 workshop held in Rome on May 14th -15th 2012, through a Focus Group with external experts with different backgrounds. A former airline security manager, a security instructor certified by IATA and ECAC and the security director of an Italian airport were present.
Many different Security issues were identified and discussed.
In particular, we identified a set of security measure that can vary in time or from country to country in their implementation, always being compliant with International and National legislations. In Figure 5 a diagram is drawn to describe the high-level scenarios relevant issues and decision-making process.

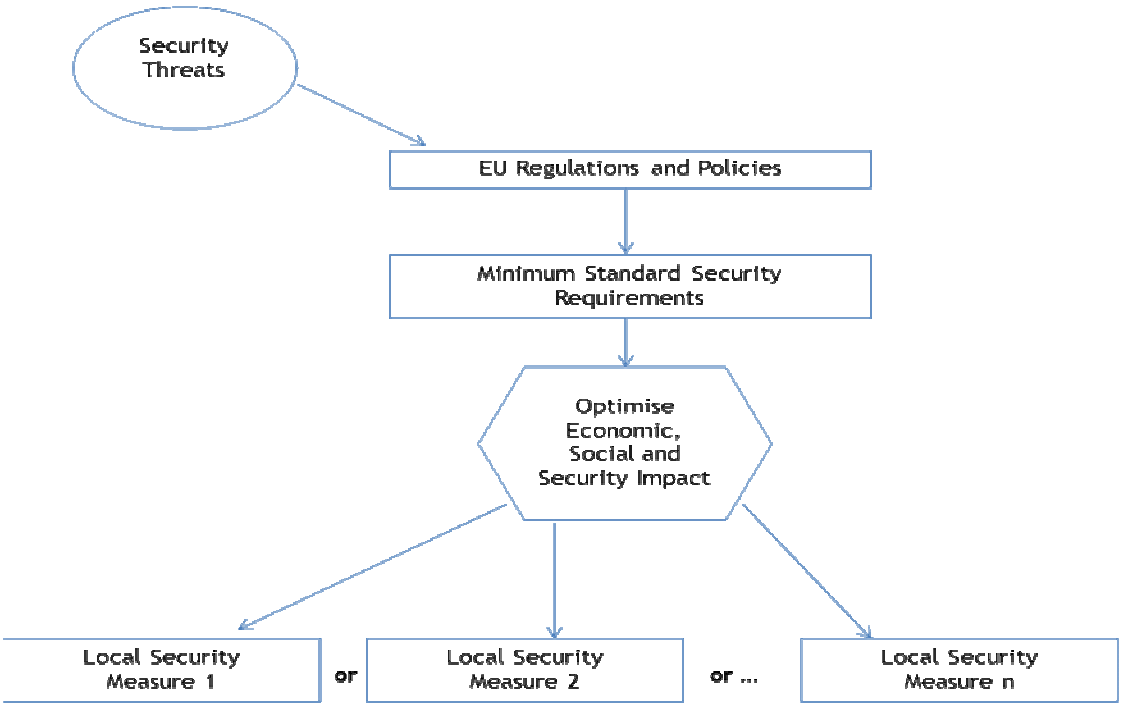

Figure 5 - High-level Scenarios' Decision-Making Process in the Airport Case Study.

In Table 3 we provide a first list reporting some high level security measures relevant for SECONOMICS analysis and scopes.

Table 3 - Preliminary set of high-level scenarios identified.

Identity Control	Differences between countries in terms of security checks frequency and ID/passport control on national flights (when not stated by the law)
Security Check	Tuning of security check: different possibilities (x rays, metal detectors, dogs, number of operators, random controls, etc)
Security Restricted Area	Airport in a protected area, less controls. Before, much more controls on the airside. Critical part of security restricted area (in small airport not mandatory)
Transit	One stop security – no double security checks (depending on countries)
Training	More or less training days for organisation employees Should we train more pilots or people on ground? Shift costs from an actor to another one, or reduce costs globally?
Profiling	Pointing out strange behaviours and unusual events could be an important component of the security system; all members of personnel should be trained with psychology techniques.
Baggage-Passenger Reconciliation	Every baggage is linked with a passenger: is it possible to remove the last control (baggage ready to be load on the aircraft), which can be expensive in terms of time and cost, considering the many and accurate security checks?
Pre-check Area	Crisis events happened mostly in these areas, easily accessible by everyone, where the security controls are held

	only by Public Police Officers. In these areas a well-defined security control point has not yet been identified.
Body Scanner Introduction	BSs have been introduced as a Passenger screening system, due to the weakness of WTMD to detect non-metal weapons and explosives hidden on the body. Drawbacks: cost, privacy, health issues, effectiveness

This preliminary list was further discussed and analysed with the Security experts and consortium members and prioritised accordingly to their operational impact for the Aviation domain, their economic and social impact as well as to their suitability and relevance for SECONOMICS research.
Finally three high-level Scenarios were selected. The first one is about the Passenger - Baggage Reconciliation procedure, the second one analyses the Introduction of Body Scanners, while the third one concerns Security Training for Airport Organization Personnel.
A common template has been defined to describe the scenarios.
Template legend: "*Scenario description*" gives an overview of the selected scenario; "*Impacts*" shows which is the impact on airport life, passengers, organisations, etc. "*System/Agents involved*" shows which component of airport system/personnel is involved (security officers, whole personnel, etc.). "*Perpetrators*" points out who can violate the security measure; "*Countermeasures*" shows which possible actions the airport organisations can implement to resist to perpetrators attacks. "*Not applicable*" means that the particular field does not suite for the nature of the selected scenario.

3.2.1. Passenger - Baggage Reconciliation

Scenario description: the 'reconciliation' between the passenger and baggage is defined by most air transportation authorities, such as the US Federal Aviation Association and the European Union's Joint Aviation Authorities : "a key measure in preventing acts of unlawful interference and shall be applied in addition to other types of control."
This security procedure ensures that no luggage would travel without the corresponding passenger because the luggage might contain a potential bomb. Making sure passengers board flights onto which they have checked baggage in is a complex process called "passenger-baggage reconciliation" and is accomplished semi-automatically through various commercially available systems and through the involvement of specialised front-end personnel.

Impacts: the passenger – baggage reconciliation became a mandatory procedure in the late '80s, after terrorist bombing attacks in which unaccompanied suitcases led to the downing of two flights, when a bomb inside the suitcase exploded.
The two famous terrorist incidents were respectively:

- In 1985, the *Air India Flight 182* incident. *Air India Flight 182* was an Air India flight operating on the Montreal–London–Delhi route. On 23 June 1985, the aircraft operating on the route — a Boeing 747-237B (c/n 21473/330, reg VT-EFO) named after Emperor Kanishka — was blown up by a bomb at an altitude of 31,000 feet (9,400 m), and crashed into the Atlantic Ocean while in Irish airspace. A total

of 329 people were killed, including 280 Canadians, 27 British citizens and 22 Indians. The incident was the largest mass murder in modern Canadian history, and the deadliest aviation disaster to occur over a body of water.

- In 1988, the Pan Am Flight 103. *Pan Am Flight 103* was Pan American World Airways' third daily scheduled transatlantic flight from London Heathrow Airport to New York's John F. Kennedy International Airport. On Wednesday, 21 December 1988, the aircraft flying this route, a Boeing 747-121 registered N739PA and named "Clipper Maid of the Seas", was destroyed by a bomb, killing all 243 passengers and 16 crew members. 11 people in Lockerbie, in southern Scotland, were also killed as large sections of the plane fell in the town and destroyed several houses, bringing total fatalities to 270. The event is also known as the Lockerbie bombing.

After these two major terrorist attacks, the reconciliation procedure seemed the only possible solution to avoid on-board bombs. The security presumption of passenger-baggage reconciliation was that terrorists don't want to kill themselves, and would not board on an aircraft if they have placed a bomb in its hold. The reconciliation security measure would obviously not prevent 'suicide bombers', but could in principle prevent many different attacks and save millions of lives.

According to the reconciliation procedure, if a passengers flying with (an already) *checked-in* baggage and fails to arrive at the departure gate before the flight is *closed*, that person's baggage must be retrieved from the aircraft hold before the flight has the permission to take off. If this happens, aircraft take-off is delayed, causing rescheduling and problems to passengers and airlines.

Moreover, also in 'standard conditions' (without any abnormal event to deal with) the overall reconciliation process involves several procedural steps and different organisations and it is very complex and expensive. The baggage reconciliation procedure is supported by a resource and effort consuming technical and procedural infrastructures.

System/Agents involved: a baggage reconciliation system should be able to manage the process of passenger-baggage reconciliation for airports of all sizes. Sensors and software tools should provide real-time information to handlers, airlines and airport operators while making the baggage management process more efficient. The system should support the following operations: baggage tracking and sorting, passenger information management and distribution, checking of passenger and baggage status in real time and alerts provision to the front end operators.

After the 11th September 2011, the security level of civil aviation increased, new rules and procedure took place fostered by new technologies and detection machines. The 100% electronic screening of all checked baggage became mandatory in all countries.

The passenger-baggage reconciliation became, in some sense, redundant and some National authorities started to review it and lower its application standards.

For instance, in the United States, the passenger-baggage reconciliation is not applied anymore to domestic flights since all bags are required to go through explosive detection machines (EDS) and thus are '100% secured' prior to loading.

SECONOMICS aims to analyse and evaluate the actual cost and benefits of the passenger-baggage reconciliation, taking into account all the relevant aspects of aviation system security level and overall efficiency, economic impact, passenger facilitation and social acceptance.

We would also identify possible alternative or 'mixed' solutions, trying to assess their economic viability and operational feasibility, in order to provide useful insight and input to European Aviation Authorities and National Regulators.
Perpetrators: not applicable.
Countermeasures: not applicable.

3.2.2. Full-body scanner

Scenario description: "a full-body scanner is a device that creates an image of a person's naked body through their clothing to look for hidden objects without physically removing their clothes or making physical contact" (http://en.wikipedia.org/wiki/Full_body_scanner).
It was 1992 when this technology had been developed, but it was only 2007 when the first machine was implemented in an airport: Schipol (Netherlands) started to implement the device in large scale, after testing it on the personnel for one year. Since then many airports, especially in US, decided to buy the device and by the end of 2010 TSA (Transport Security Administration, US agency created after the 9/11) reported that there were 385 full-body scanners, 68 just in United States airports.
There are two types of this machine: the *millimetre wave scanner* and the *backscatter X-ray*.
The former is a whole-body imaging device used for detecting objects concealed underneath a person's clothing and it comes itself in two varieties: active and passive. Active scanners direct millimetre wave energy at the subject and then interpret the reflected energy. Passive systems read only the raw energy that is naturally emitted from the human body or objects concealed on the body. With active scanners, the millimetre wave is transmitted from two antennas simultaneously as they rotate around the body. The wave energy reflected back from the body or other objects on the body is used to construct a three-dimensional image, which is displayed on a remote monitor for analysis. The passenger walks and stops inside the machine, waiting for the scan for about three seconds. During this time, the machine creates a 3D image, as explained above, and it is displayed directly on a screen outside of the device: the image consists of a generic outline of a person for every passenger; at this point, if no threat is found by the internal processor of the machine, a green sign appears on the screen and the person is free to move on.
Impact: the backscatter X-ray technology is based on, a form of ionizing X-rays and detects the radiation that reflects from the object and forms an image. In contrast to millimetre wave scanners which create a 3D image, backscatter X-ray scanners will typically only create a 2D image (for airport screening, images are taken from both sides of the human body); the image is displayed on a remote screen, controlled by personnel closed in a separate room and he/she cannot see the identity of the passenger. In case the result of the scan is positive, the officer in the remote control room highlights the report to personnel at the security checks and the pat-down can be performed. In some cases, this type of machine can be found in another layout: the passenger, after passing the usual metal detector, passes through the full-body scanner, and the image is displayed directly on a screen close to the machine (this is the layout the Italian airports are going to use).
The choice between different technologies and among different layouts and subsequent operational procedures will modify the overall airport security level strongly affecting the passenger security perception. Moreover, airport organization, processes and work

practices as well as costs and infrastructures may vary significantly according to the selected body-scanner technology and foreseen implementation.
There are two big issues with full-body scanners: health and privacy.
For what may concern the health, TSA states that the energy projected by millimetre wave technology is thousands of times less than a cell phone transmission. A single scan using backscatter technology produces exposure equivalent to two minutes of flying on an airplane, but delivered in few seconds. On the other hand, the backscatter X-ray technology, based on ionizing X-rays, can damage chemical bonds and be carcinogenic, if used in big doses, which is not the case of passengers at the security checks. It is important to highlight that the procedure is not compulsory in all the countries: in USA passengers can opt out and decide to pass through usual machines, such as metal detectors, which can be equally dangerous (or even more) than the full-body scanners. The European Commission also recommended that alternate screening methods should be "used on pregnant women, babies, children and people with disabilities".
Privacy: full-body scanning technology allows screeners to see the nude surface of the skin under clothing (including breast prostheses and prosthetic testicles or other medical equipment normally hidden), which may lead to a potential embarrassing considering a pat-down. In the beginning of the project, several screeners had been caught reviewing the images, which are *not* supposed to be stored (the function is disable by the manufacturer companies), and the perception of the passenger is related with possibility to be seen naked by officers.
Nowadays, in many countries, full-body scanners are not mandatory, but in a very short future they will be, and health and privacy issues have to be solved.
Some opponents state that the full-body scanners are ineffective, as reported by an Israeli airport security expert, because they cannot detect bombs or other weapons, if they are attached to the clothes: in this way, the object should be on the black background of the image created by the machine. It is important to remind that with the introduction of full-body scanners the pat-down cannot be performed, unless the alarm is displayed on the screen. This has also been proved by several viral videos posted by a US engineer on March 2012.
Agents involved: Security Officers (Screeners).
Perpetrators: Passengers with malicious intent.
Countermeasures: not applicable.

3.2.3. Training

Scenario description: despite advances in technology in airport security, there is no substitute for highly trained and qualified personnel. In the aviation security industry, technology is only one layer of security, and human factors in security cannot be overlooked or minimized.
Over-reliance on technology is a trap that leaves passengers, aircrews, and airport personnel vulnerable to a terrorist attack. Thus, security training for Airport Staff is a central issue in ensuring and maintaining a high level of Security in airport environment.
Airport security has long been considered an important issue, but has become even more so since the 9/11 terrorist attacks. Effective airport security does not stop with well-trained and efficient Security Personnel. A *'Security Culture'* is established when all airport employees are conscious about security problems, understand crisis management and how to report crimes, security breaches and suspicious activities.

Nowadays, security training is a required component for all airport personnel, from airport security officers to truck drivers and custodians, with a need for unescorted access. Individuals are trained to recognize and act upon certain security breaches.

Agents involved: training is specifically designed for each type of employee position within the airport. For example, transportation security personnel are trained to properly screen passengers, luggage and cargo. Security personnel learn about the recognition and handling of explosive devices, as well as X-ray screening. A logistics truck driver will be trained on cargo handling and security.
Professional security, especially in the aviation industry, requires special skills, knowledge and abilities. Security training at airports varies according to security employee positions. Security Operators (screeners) learn how to screen baggage and passengers, while higher-ranked Security Officers learn supervisory skills so they can oversee employee training and scheduling. Supervisory Security Officers are trained to deal with cargo and baggage security. Finally, Airport Security Managers learn management techniques to oversee the screeners.

Impacts: analytical and critical thinking abilities to solve problems should be crucial points of personnel training. Unfortunately, technological and chemical advances are resources of terrorism. Security personnel must have the ability to identify potential elements of improvised explosive devices.
Other critical abilities of an airport security professional include the detection of questionable behaviour ('profiling activity'), interpersonal communication to be proactive in quickly developing a rapport with people in order to determine whether or not an individual may be involved in terrorist activity, and how to assess multiple threat possibilities. In-depth, knowledge of world cultures, global affairs, terrorism and counter-terrorism, and foreign languages should be automatic qualifications for individual working in airport security. If an individual does not have this education and knowledge, they should not be working in the aviation security industry. Merely showing security personnel a short training video about culture and terrorism is grossly inadequate. The hiring of unqualified personnel is the first step in the defeat of a multi-tiered security operation.
The training of airport security officers today needs tremendous improvement. Live training scenarios are crucial for successful security operations. Simply watching a video or taking computer based tests of explosives and terrorist attacks does not make a security officer qualified to do the job. This appears to be the current trend in airport security training. Security personnel must clearly understand all elements of possible improvised explosive devices and what proper action to take in order to save lives and aid in the apprehension of a terrorist. The only way to obtain this knowledge is through extensive and continued training and education from *qualified* and *experienced* instructors. The aviation security industry needs to be constantly open to adapt to changes quickly to the ever-evolving threats of terrorism.
Unfortunately, airport security today is more reactive than proactive. For example, after the "shoe bomber" incident (occurred on December 22, 2001 on Flight 63 from Paris to Miami), passengers now need to remove shoes going through a security checkpoint.
In the Christmas 2009 an attempted terrorist attack on board Northwest Airlines Flight 253, en route from Amsterdam to Detroit was carried out by Umar Farouk

Abdulmatallab, an Islamist terrorist. The liquid explosives this individual had concealed on his person were not detected during security checks. After this incident, security experts claimed if a full-body image scanner was used, this incident would have been avoided. But a full-body scanner is only one layer of security. Again, technology is important, but it cannot be left to be a single point of detection. All other steps to a successful security system such as profiling and professionally trained personnel to question and interact with passengers are equally, if not more, important.
It should be noted that the preservation of human rights and privacy can be maintained, and it is important to understand that methods of an effective security system are designed to save lives and capture terrorists.
There are strides being made in the right direction regarding increasing standards of airport security personnel.
Possible alternatives and choices are:
Improving Airport Personnel Skills
1) Raise hiring standards to include higher academic requirements in the following areas: Global affairs, foreign languages, intelligence, psychology, counter terrorism or homeland security. Another critical skill is analytic ability. Hiring efforts should also reduce the number of supervisors and increase the number of operational professionals. Professionals are able to make decisions on their own, without going through a long supervisory chain of command that passes on the decision to be made by someone else. Hiring true aviation security professionals also requires an improved employment compensation package to recruit and retain individuals with above average skills, abilities, job duties, and qualifications. By hiring and retaining quality individuals, financial resources can be applied to other areas, rather than the constant hiring and training process present in today's security field due to a very high-turnover rate.
2) Provide more advanced security training to all airport personnel including ticket agents and baggage handlers. This would be another layer of security that can be integrated into one security system that goes above and beyond perimeter security, surveillance, and presence of law enforcement and military personnel.
3) An effective and simplified process is needed in order to enhance communication and sharing of intelligence information between airport organizations and security agencies.
4) A longer, more comprehensive training program for airport security personnel that includes live training scenarios, Improvised Explosive Device (IED) detection, counter-terrorist tactics, etc. Furthermore, training should be on a continuing basis at least monthly. It is also absolutely essential that aviation security professionals are proficient with any equipment used on a daily basis, or other equipment used in the event of an emergency situation.
5) Amend international regulation and national laws to give aviation security professionals more authority than merely "observe and report." This level of response needs to be amended to allow security professionals to "observe and protect." For example, any unusual situation requiring immediate action, security professionals must be able to handle the situation. Shutting down airport operations scares passengers while waiting for law enforcement to arrive seems to be the current tactic used in airport security, which is very unprofessional.
6) Raise standards of physical fitness that involve an agility test equivalent to any other government agent or law enforcement position including defensive tactics and firearm training. Combat Sambo has been proven to be the most effective defensive tactics because it is relatively easy to learn in a short time, which maximizes resources.

7) Learn from other models of airport security such as the Israeli example. Here the profiling is one the most used counter terrorism techniques, but it is integrated with passengers data, always available for security officers, and with travel history: the ground crew, at the check-in desks, has to be trained to recognise strange situation just from the passenger travel history. The final goal is to train personnel in order to increase the number of security officers, spread around the whole airport area.
8) Qualified instructors should have credentials that include special operations experience, international government agent experience and an intensive counter terrorism security background.
Improving Aircrew Skills
1) Provide more advanced security training to flight attendants and pilots including observation and detection techniques (enhanced profiling for everyone's security)
2) Basic Improvised Explosive Device (IED) detection and the various forms used such as everyday objects like a pen.
3) Defensive tactics training: a) self-defence b) defending a third party c) how to properly detain an aggressor.
4) Provide basic hostage negotiation training.

An important additional improvement would be the enhancement of the communication process and information sharing between airport and 'airline' sides, involving post-security check and boarding phases. Recent laws stated that the personnel working inside the airport area must wear the ID badge, to be recognise in every moment by security officers, and that it is compulsory to report if anyone is not wearing it: again, a security culture has to be understood by the personnel, in order to prevent conspiracy of silence between the personnel itself.
Security has a huge economic impact on the airlines companies, and thus on the passengers. A normal consequence, in order to "survive", is to cut the training costs (less hours and less skilled instructors), leading to possible holes in the security. A possible solution is to increase the training for the other stakeholders (airport and handlers) personnel, permitting the airline companies to reduce the amount of money dedicated to the training, keeping high security standards.
Perpetrators: not applicable.
Countermeasures: not applicable.

3.3. Airport Security Operational 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 are fictitious to preserve confidentiality and for security reasons. The study is structured in a way that an AO may insert their own details and undertake their own computations if required. In the figure below a diagram summarizes local operational scenarios rationale and scopes.

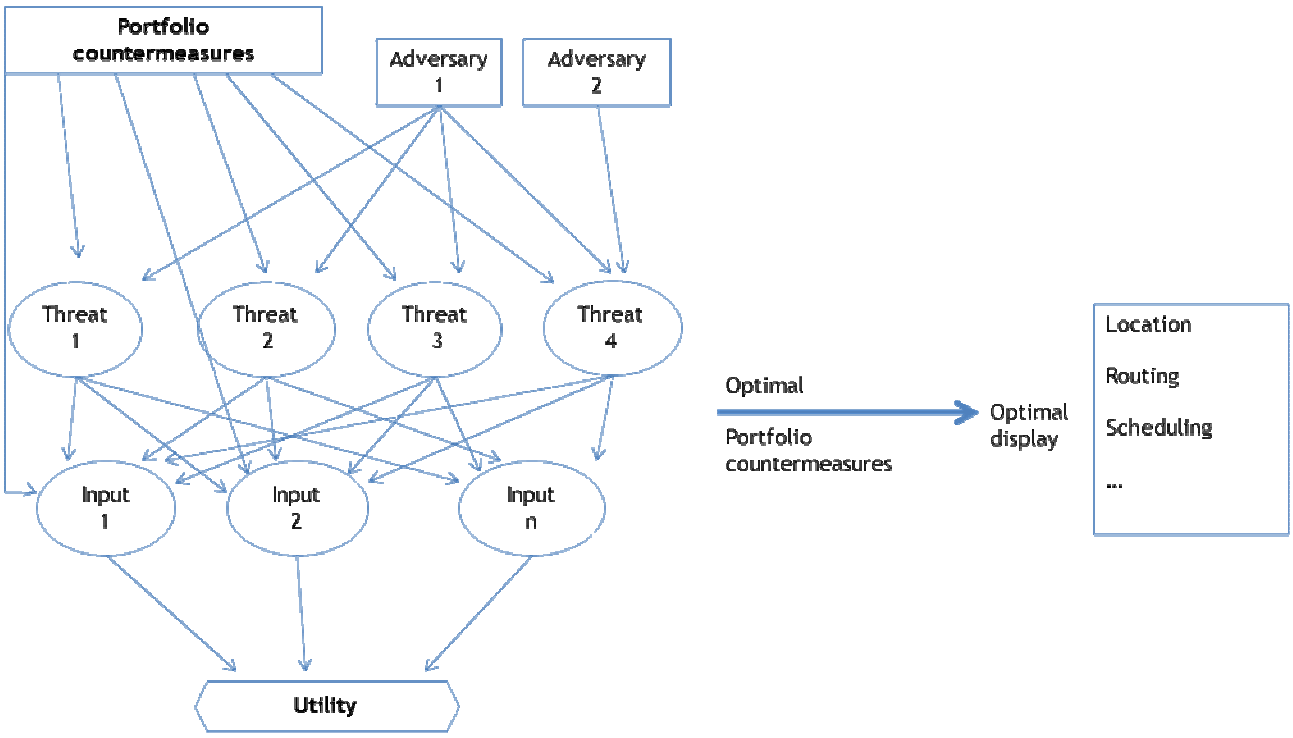

Figure 5 - Operational Scenarios Modeling in the Airport Case Study.

3.3.1. Description of Anadolu Airport

Anadolu Airport (AA) is operated for both international and domestic flight within flight training operations. Airport general facilities are:

- Single runway flight operations,
- Runway 3000 x 45 meters,
- Runway lighted for night flights,
- Radio navigation aids: VOR, DME, ILS, NDB,
- Terminal and technical facilities such as ATC, AIM and meteorology.

The manpower of the airport that is responsible for the airport terminal, tower and technical facilities, navigational aids, airside and airport vehicles is totally 150 people. They are following the work shifts depending on the international flight schedules.
The enclosed Table 4 lists the relevant data concerning current security resources.

Table 4 - Relevant data concerning current security resources in AU Airport.

Number of security (private)	Number of airport police	Number of sniffer dogs	Number of cameras	Number of Watching Towers
70	20	2	50	6

Terminal security resources are X-Rays, gate detectors and cameras.
Airport police and armed private security personnel are responsible for normal security operations together such as gate and passport checks for passengers and luggage checks. In any case of security threats, they act as first security agents and immediately call

main police centre of the airport city. Their responsibility is limited with securing and saving people and facilities involved under any negative situations. In case of security threats, special police force takes management of the situation. They have special action plans depending on the situational requirements.

3.3.2. 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.
It is especially concerned with several threats described below. Most of them are 'traditional' but they have seen an increase in rate of occurrence, some of them are fairly recent. They have also identified several potential threats. Some of them affect directly the business; others potentially affect business through image deterioration.
The airport has a developing potential for both flight training and domestic and international air travel. When any potential risks occurred, security perception of people can be damaged as air travel on the airport is hazardous. This image can create additional security barriers and investments/costs for the airport. 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.
Given the situation, the management of AA airport can create a budget when required for the security needs during the operation year.

3.3.3. Threats and impacts

The security observations and analysis identify the following weaknesses are:

- Airport border fences are very close to civil public area.
- Insufficient terminal design.
- Same entrances and roads are used for both public and airport in the field.
- Concerts, sport challenges and festivals are held in the field.
- Experience of security personnel.

The weak points about airport security can be used creating scenarios. Through several meetings and data analysis the following scenarios have been identified including multiple weaknesses.

3.3.4. Scenarios

In this study, 4 security scenarios were created to discuss on the airport security and results. These are:

- Unlawful Access to the Tower and Interference to Tower Operations
- Unlawful Interference to Apron
- Unlawful Interference for Airside
- Unlawful Interference in Terminal Security Checks

3.3.5. Unlawful Access to the Tower and Interference to ATC Operations

Scenario Description: The airport ATC Tower is attached to the terminal building and its gate is located in the main lounge of terminal. A person among the passengers can plan to enter tower and to take hold of air traffic controllers before or during the flight control operations. He/she somehow could find an opportunity for tower entrance gate

and goes up to tower. He/she can 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. 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. Beside the safety and security impacts the cancellation cost can be enormous with the connected 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.
Perpetrator: Somebody who is a member of any ethnic/politic body.
Countermeasures: Cameras.

3.3.6. Unlawful Interference to Apron

Scenario Description: The closest point of the security fences near to terminal and apron could be used for fixing a harmful object/tool by throwing/sending over the fences some time before or during the flight operations. This can give an opportunity to threat flight operation people and passengers when boarding process.
Impacts: Loss or injury of people, aircraft, airport vehicles and terminal building, crisis for air traffic operations in the air field and airspace. Apron is blocked.
All flight operations are cancelled. The cancellation cost can be enormous with the connected flights and airports/airspace.
A result will be negative security perception for airport users. As a result of this interference people image can be affected negatively.
Media can inform people immediately about the situation. This can cause new crisis around the airport facilities and operators.
Agents: AA. Private security and airport police, flight crew and operators at the apron.
Perpetrators: Attackers for their politic objectives.
Countermeasures: Fences.

3.3.7. Unlawful Interference for Airside

Scenario Description: The closest border of security fences to the public area can be entrance location for a person who plans any harmful interference for flight operations. He/she can enter the airside and fix some harmful tools/objects to airside facilities during the night time. This interference may result hazardous situations for flight safety and airport security. For instance any objects can damage landing gears of any aircraft located on the touchdown.
Impacts: Loss or injury of people, aircraft and navigational aids. Runway is blocked and all flight operations are cancelled until the investigations were performed.
Negative security perception for airport users. As a result of this interference people image can be affected negatively who are travelling by air.
Media can inform people immediately about the situation. This can cause new crisis around the airport facilities and operators.
Agents: AA. Private security, runway safety team, air traffic controllers.

Perpetrators: A young/drunk person who wants to protest any situation.
Countermeasures: Fences, security watching towers.

3.3.8. Unlawful Interference in Terminal Security Checks

Scenario Description: The first security point of terminal can be used to fake of security personnel. This situation can be provided by creating conflict when entering point is crowded and security personnel are busy. In this way harmful goods/objects can be passed into the terminal and cabin.
Impacts: Loss or injury of people, aircraft, airport vehicles and terminal building, crisis for air traffic operations in the air field and airspace.
All flight operations are cancelled. The cancellation cost can be enormous with the connected flights and airports/airspace.
Negative security perception for airport users. As a result of this interference people image can be affected negatively who are travelling by air.
Media can inform people immediately about the situation. This can cause new crisis around the airport facilities and operators.
Agents: AA. Airport police and private security.
Perpetrators: Attackers who wants to create big negative effect on people.
Countermeasures: Cameras, X-Rays and gate detectors.

4. Airport Security High-level Operational Requirements

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 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 [7], 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. State Members can create a different organisation, as European Union Members did, creating the EASA (European Aviation Safety Agency). EASA 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, EASA issued several different laws, which have been modified and amended, and nowadays the most important are the REGULATION (EC) No 300/2008 [1] and the COMMISSION REGULATION (EU) No 185/2010[2]. 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 [1] 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).
In this 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 NPS in order to check the level and quality of civil aviation security within its own territory, at the same time complying the EASA 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.

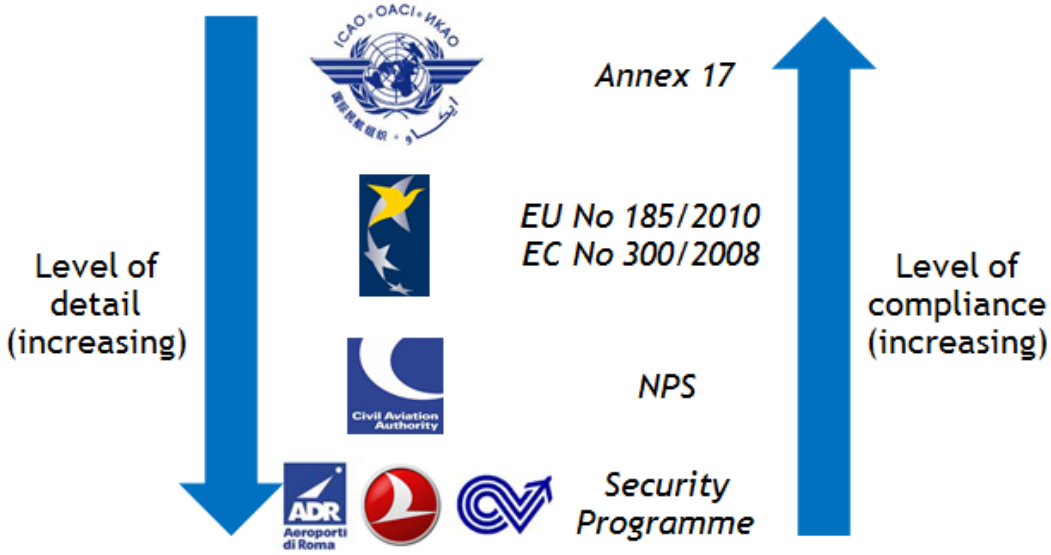

Figure 6 - Worldwide, European and National Regulations.

Figure 6 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. Chapters 6.1, 6.2 and 6.3 show in detail where to find rules, laws, regulations, etc. and a brief description is given

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.

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 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 [4], art1.

ECAC made identifications about aviation security in its Document [6], 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 [7], 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;

The ECAC Doc 30 [6] Part II also made some explanations about security examination methods. These are:

Hand search: A hand search should consist of a thorough manual check of the areas selected, including contents, in order to reasonably ensure that they do not contain prohibited articles. *[2] Annex 1.4.3.1*

Areas to be hand searched or visually checked. A search by hand should be performed for the examination of areas referred to in points a), b), c) and f). A visual check may be used as an alternative method of examining those areas when they are empty. [5] Annex 1.4.7.
A visual check should be applied for the examination of areas as referred to in points d) and e). [5] Annex 1.4.8.

Supplementary means of examination: The following methods may only be used as a supplementary means of examination:

a) Explosive detection dogs; and
b) Explosive trace detection (ETD) equipment. *[2] Annex 1.4.3.2*

ECAC DOC 30 Part 4 identifies issues about airport security as below:

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. [*2] Annex 9.0.1.*

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. [1] *Annex art9.*

Application: Airport supplies should be screened before being allowed into security restricted areas, 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 taken into the security restricted area. [*2] Annex 9.1.1.1.*

Airport supplies originating in the security restricted area Airport supplies which originate in the security restricted area may be exempted from these security controls. [*2] Annex 9.1.1.2.*

Visual check of airport supplies: Upon delivery at the outlet in the security restricted area, a visual check of the airport supplies should be carried out by the staff of the outlet in order to ensure that there are no signs of tampering. [*2] Annex 9.1.1.4.*

Airport supplies showing signs of tampering: Any airport supply received from a known supplier that shows signs of being tampered with, or where there is reason to believe that it has not been protected from unauthorised interference from the time that controls were applied, should be screened. [*2] Annex 9.1.1.3.*

Screening: Appropriate screening methods. When screening airport supplies, the means or method employed should take into consideration the nature of the supply and should

be of a standard sufficient to reasonably ensure that no prohibited articles are concealed in the supply. [*2] Annex 9.1.2.1*.

Methods of screening: When screening airport supplies the following means or method of screening, either individually or in combination, should be applied:

a) Visual check;
b) Hand search;
c) X-ray equipment;
d) Explosive detection systems (EDS) equipment;
e) Explosive trace detection (ETD) equipment; and/or
f) Explosive detection dogs, in combination with a)

All these methods are reported in [5] Annex 9.1.2.

4.3. ECAC Identifications for Air Traffic Management Security

ECAC Doc 30 includes Air Traffic Management security in its chapter 13 as following [*Ref DGCA/133*]:

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.

5. Modelling the Airport Case Study

A first set of possible modeling approaches developed in WP5 and WP6 and preliminarily applied to the Airport Security Scenarios are reported in next paragraphs.
In the D1.3 deliverable they will be further detailed and integrated, while first examples of specific models and results will be presented.

5.1. Game Theoretic Approach

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. Positive externalities exist when security investments of an agent decrease the security risks of other agents. In contrast, a negative externality exists when an agent's increased security investment raises the security risks of other agents. 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. Specifically, the airport security involves high-level complex security systems and extremely heterogeneous stakeholders (e.g., airports, airlines, government agencies and supranational institutions), and security in an airport depends on the security performance of other airport (e.g., the explosion of Pan Am 103). This implies that airport security is not only beyond the abilities of an individual airport but also extremely complex and dynamic: in order to guarantee the global functionality of security in airports, 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 heterogeneous stakeholder should work in a cooperative and interactive manner, and coordinate its security actions with other airports: the stakeholders such as airports and airlines need to work together toward satisfying a large set of joint goals, and policy-makers such as governments and supranational organizations need to develop in advance protocols and regulations for coalition among the stakeholders.
We believe that an interdisciplinary approach based particularly on game-theoretic techniques is suitable for studying a broad class of coordination and cooperation issues in the airport security. Game-theoretic models use mathematical techniques for tackling conflict and cooperation issues between agents. While game-theoretic models can be divided into two types (i.e., non-cooperative vs. cooperative models), we will focus mainly on cooperative situations where the agents involved in security within an airport and between airports cooperate to increase the security functionality. For example, airports might have different security measures, different costs associated with the security measures and different security capabilities. In this situation, although each

airport can act independently and reach its security goals by itself, the airport may want to join together and form coalitions in order to gain greater security functionality. Cooperative game-theoretic models provide us with a good framework in the development of the coalition formation between agents involved in airport security.
In applying the game-theoretic framework, 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.

Motivation and Attitude
Regarding airport security, a broad range of technical security solutions, ranging from simple screening technologies to complex full-body scanners, is increasingly employed. However, in investigating several airport security cases, we identified that the ineffectiveness of various security controls is not only caused by the limitations of these solutions but also by inadequate use of them.
Since most of the employees may not suffer directly from damages caused by security accidents and have limited incentives to work hard for preventing security risks. Furthermore, since employees derive disutility from effort to increase security functionality, they will be adverse to exert proper effort levels. In contrast, an employer cannot observe an employee's efforts for reducing security risks and, due to costs of monitoring, cannot verify whether the employee behaves properly. In addition, because of the interconnected nature of security environments, airport security needs teamwork. Teamwork makes it more difficult for the employer to determine the employee's contribution to system security and a correlated payoff, which provide the right incentive to him/her (i.e., the problem of misaligned incentives and moral hazard). These factors give employees incentives to shirk the contracted effort for security.
Based on a behavioral framework, we will analyze whether ineffective implementation of security measures is largely caused by poorly motivated employees (i.e., a moral hazard problem) and whether it can be overcome by providing appropriate motivation: that is, offering training programs.

5.2. The Risk Analytic Framework

The Airport Case Study will be solved within the risk analytic framework. To do so we shall proceed as follows:

- Indentifying the management objectives of the case study owner, as far as the case study is concerned.
- Identifying the relevant threats to be considered in the problem, a detailed description, underlying motivations, involved agents, interactions.
- Assessing the risks associated with such threats. This entails assessing their probability of occurrence, describing their impact and the impact distribution, assuming that the threat happens.

- Identifying the countermeasures and how do they impact the various threats, i.e. how do they reduce the likelihood of occurrence of such threats and/or how do they mitigate the effects, should they occur.
- Identifying various constraints, including the budget available for risk management, legal constraints in reference with countermeasures, e.g. stemming from ICAO, and so on.
- Formulating the utility function for the problem at hand, identifying the tradeoffs between various objectives, as well as the impact of risk perceptions on the utility function. We shall consider not only attributes in connection with costs and security, but also in relation with convenience and comfort for airport users.
- Finding the optimal risk management portfolio, which is the one that maximizes expected utility, while satisfying the constraints.
- Communicating the risk management portfolio and describe how the impact of such portfolio may be monitored.
- Once with the optimal portfolio, we shall study optimal deployment of resources, e.g. optimal (random) routing of patrols.

The problem might seem at first sight as based on a standard risk approach but four features may require introducing novel methodological features:

- The explicit introduction of issues in relation with risk perception may require novel features in preference modeling.
- The adversarial nature of the problem, with several of the threats having a clear intentional nature. This requires trying to forecast such intelligent driven and adaptive activities, thus entailing developments from the recent field of adversarial risk analysis. Note that we have identified several possible groups performing the threats, and some of them might have clear political motivation.
- The underlying structure of the problem, which is a special setting with several installations within the space with special value.
- For some of the threats, we might need to heavily use subjective probability assessments given the lack of data.

Once solved the problem, their essential features will be extracted to develop templates for solving similar problems in the future and for deploying within the SECONOMICS tool.

Annex – Airport Ethnographic Study

Example of questionnaire:

- Which is/was your role in Your Organisation?
  - Responsibilities/Tasks
  - Which external organisation and internal function do/did you work with more frequently?
- What is/was your interface/link with Airport Security?
- Which is your background?
- Which are your previous experiences?
- Which should be the role of Your Organisation inside the airport?
  - Responsibilities/Tasks
  - Activities
- Area of Activity (e.g. Hangar, Management offices, front-desk, gate,…)
- Background of involved personnel
  - Profile, expertise, security competencies
- What is the relation, in terms of security, of your organisation with the other airport stakeholders?
- Which is the relation between Safety and Security?
- Can you give us 3 hot topics, in terms of Security?

Record of experts, divided per organisation:

- **ANSP**
  ENAV Information Security Manager:
  - ENAV Security Operation Centre to monitor ALL the logical and physical threats for the operational, central and business unit (ERP).
  - Risk Assessment of ENAV Company.
  - Design a Secure Network Infrastructure compliant with SWIM and SESAR.
  - Participate to R&D projects on Security.

  Open Issues for an ANSP:
  - Correlation among physical and logical events (example: badge & access)
  - Data integration: temperature of server rooms & possible incidents, access control & work schedule. Proactive risk monitoring.
  - From physical to logical/IT security in airports:
    - Airport Collaboration Decision Making: new system in big airports to share data and info in real time.
    - Today on-line flight plans , before by fax
  - Relation between Safety and Security.
  - Security Cultural Problem: no training, no commitment, too many sub-contractors and third parties.

- **Air carrier**
  Former Alitalia Security Manager and ENAC Security Instructor:

- 20 years in Carabinieri – counter-terrorism dept.
- 20 years Alitalia Security Manager:
  - Member of the inter-ministry security committee
  - Member of international committees for ICAO
  - Internal training projects
- ENAC certified Security Instructor:
  - courses for all airport personnel

Open Issues for an Airline:

- Security during transit in big hubs.
- Security and efficiency (from arrival to new departure of an aircraft: 30 minutes – too many operations!!).
- Security Culture of many operators and not qualified personnel (third parties, temporary contracts, etc.)
- No dedicated and secured areas for server rooms.
- Cargo Security: freights security is a very important and specialised issue. *Involve DHL, UPS or another shipping & logistic company.*
- Security policies and regulations are 'top-down'

- **Airport Operator**

ADR Security manager

- 3 years in Carabinieri – FCO
- In ADR since 2002 (Graduated in Law):
  - Trainer
  - Operative responsible for Ciampino and Fiumicino

Open Issues for Airport operator

- Training: more than 1000 people working for the company → there is the need for a new programme with less impact on costs and operative capacity of the personnel (training on the job for screeners is on at the moment, with projected bomb and weapons images on the screen).
- Infrastructure: there must be a foresight of the airport growth, in order to understand the limits and possible inconveniences for passengers
- Information circulation: a big company needs to have better technology for the personnel to communicate internally (towards colleagues) and externally (towards the other airport providers)

REFERENCES

[1] EC Regulation No.300/2008, European Commission, 2008.
[2] EC Regulation No. 185/2010, European Commission, 2010.
[3] EC Regulation No 2320/2002, European Commission, 2002.
[4] EC Regulation No. 1254/2009, European Commission, 2009.
[5] EC Decision No. 774/2010, European Commission, 2010.
[6] ECAC Resolution No.27-2, ECAC policy statement in the field of aviation facilitation, 2003.
[7] ICAO, Annex 17, Security Safeguarding International Civil Aviation Against Acts of Unlawful Interference, Chicago, 2011.
[8] ICAO Security Manual, Doc 8973, 7th Edition, 2010.