

SECONOMICS

D1.5 - Tool Validation

A. Pollini, A. Tedeschi, P. Marti (DBL), R. Ruprai (NGRID), F. Massacci, W. Shim, M. De Gramatica (UNITN), U. Turhan, B. Acikel (AU), A. Schmitz (ISST), P. Guasti (ISASCR), J. Williams (UDUR)

Pending of approval from the Research Executive Agency - EC

Document Number	D1.5
Document Title	Tool Validation
Version	1.0
Status	Final
Work Package	WP 1
Deliverable Type	Report
Contractual Date of Delivery	31.01.2015
Actual Date of Delivery	31.01.2015
Responsible Unit	DBL
Contributors	AU, UNITN, UJRC, ISASCR, NGRID, ISST, UDUR
Keyword List	Validation, tool.
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 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	 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: Dr Matthew Collinson matthew.collinson@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: Alicia Garcia Medina alicia.garcia@atos.net
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	 SOU Institute of Sociology AS CR	INSTITUTE OF SOCIOLOGY OF THE ACADEMY OF SCIENCES OF THE CZECH REPUBLIC PUBLIC RESEARCH INSTITUTION, Jiřska 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 İki Eylül Kampusu, 26470, Eskisehir, Turkey	Contact: Nalan Ergun nergun@anadolu.edu.tr
12	 Durham University	The Palatine Centre, Stockton Road, Durham, DH1 3LE, UK	Contact: Prof. Julian Williams julian.williams@durham.ac.uk

Document change record

Version	Date	Status	Author (Unit)	Description
0.1	20/10/2014	Draft	A . Tedeschi (DBL) A . Pollini (DBL)	ToC
0.2	17/12/2014	Draft	A . Tedeschi (DBL) A .Pollini (DBL) U.Turhan, B. Acikel (AU) F. Massacci (UNITN) W. Shim (UNIT) M. De Gramatica (UNITN) P. Guasti (ISASCR) J. Williams (UDUR)	First draft for WP1 internal review. Policy paper draft prepared.
0.3	22/12/2014	Draft	A . Tedeschi (DBL) A . Pollini (DBL)	First draft for project review
0.3	12/01/2015	Draft	R. Ruprai (NGRID)	1 st Scientific review
0.4	14/01/2015	Draft	A . Tedeschi (DBL) A . Pollini (DBL) P . Marti (DBL) F. Massacci (UNITN) W. Shim (UNITN) M. De Gramatica (UNITN) J. Williams (UDUR)	Second draft for 2 nd Scientific review and quality check. Policy paper revised included.
0.4	19/01/2015	Draft	R. Ruprai (NGRID) P.Guasti (ISASCR) A.Schmitz (ISST) J. Williams (UDUR)	Second draft for 2 nd Scientific review and quality check
0.4	20/01/2015	Draft	E. Chiarani (UNITN), F. Massacci (UNITN)	Quality check completed. Some minor remarks.
0.5	23/01/2015	Draft	A . Tedeschi (DBL) A . Pollini (DBL) P . Marti (DBL)	Third draft after Scientific Review
0.6	29/01/2015	Draft	A . Tedeschi (DBL) A . Pollini (DBL) P . Marti (DBL)	Fourth draft after final Scientific Review
0.7	30/01/2015	Draft	F. Massacci (UNITN) R. Raminder (NGRID)	Revised KPIs and review
1.0	30/01/2015	Final	A . Tedeschi (DBL) A . Pollini (DBL) P . Marti (DBL)	Final version

INDEX

Executive summary	5
1. Introduction	6
2. Support to Toolkit Development.....	7
2.1 Interface testing and adaptation with WP8.....	7
2.2 Tool tuning with WP5-WP6-WP8	8
2.3 Interface refinement with WP8.....	8
3. Support to Toolkit SECONOMICS Practice for Exploitation of Science-Based Policy Models.	9
4. Validation of SECONOMICS Toolkit Exploitation Practice	10
a. Validation Activities	10
b. Validation Results.....	15
5. Policy Insights from Validation	19
6. Future and Emergent Threats.....	22
7. Conclusions	23
References.....	24
Annexes	25
Annex 1 - Evaluation Questionnaire for the SECONOMICS Tool Template.....	25
Annex 2 - Final Evaluation on SECONOMICS Results Template	26
Annex 3 - Evaluation Questionnaire for the SECONOMICS Toolkit Template	27
Annex 4 - Airport Security Infographics	31
Annex 5 - SWOT analysis about the SECONOMICS tool template	37
APPENDICES	38
A. Assessment of Project KPI for the Scenario	38
B. Detailed list of Activities in Support to Toolkit Development.....	41
C. Detailed list of Validation Activities □	42
D. Detailed Tables of Results of Tool Evaluation Activities	43
E. User interaction and interface design	45
F. Detailed Tables of Results of Validation Activities	46
G. Policy Paper	48

Executive summary

D1.5 Tool Validation presents the Toolkit validation process for the Airport Security, and describes the process, the practices, the activities and the outcomes of the SECONOMICS tool validation task, including the policy guidelines and the software Toolkit for Airport Security decision support.

This report describes the final evaluation on the SECONOMICS results towards general acceptance and appreciation of the mechanisms and computational strategies under the models; the models' results quality and usefulness; and the tool implementation and effectiveness.

In WP1 the Toolkit has been introduced to the Airport Security stakeholders in different phases using the “Good Practice” approach, on how scientific models can be introduced and used by policy makers for evidence-based policy making. Stakeholders at operational decision-making level (such as Anadolu Airport, Ancona-Falconara Airport, Perugia Airport and Rimini Airport security managers) as well as policy-makers at national and international level (like Assoaeroporti, DG Move, Eurocontrol, IATA) have been involved the practice, along through four activity types: 1) Introduction and buy-in by key stakeholders; 2) Familiarization and Confidence building; 3) Calibration; 4) What-if scenario & refinement.

Stakeholders at Airport Security decision-making and policy-making levels have been involved in two workshops and also in a panel during the SECONOMICS Summit to discuss and rate the SECONOMICS Toolkit and for analyzing different security-critical scenarios. The Toolkit has been appreciated and accepted by the stakeholders involved in the final validation session. Policy-makers in the airport security domain evaluated the Toolkit as an integrated set of instruments with its own internal coherence and effectiveness.

SECONOMICS KPI for WP1 Airport Security study are presented in Appendix A and the project results are presented in the Policy Paper in Appendix G.

1. Introduction

The Toolkit validation process is a comprehensive and integrated process including the software tool and the policy guidelines implemented for the Airport Security domain. The software tool embedded both the Security Risk Model (WP5) and the Economics & System Model (WP6), first one centered on the physical attack to the tower scenario and second one on the security investment regulations scenario.

The Toolkit validation process took place during all the phases of the Year 3 activities, see table 1 for the details. In particular Phase 1 activities allowed fine-tuning and finalizing the models developed in Year 2 in order to be implemented in the software tool. During this phase WP1 offered continuous support to WP8 Toolkit development involving domain experts, security experts and HCI experts in the evaluation of the intermediate release of the Toolkit.

Phase 2 and Phase 3 instead focused on the final release of the Toolkit, both as internal and external to the consortium process. The contribution from consortium partners aimed to carry out the first exhaustive test and evaluation of the Toolkit before presenting and submitting it to the stakeholders engaged throughout the project.

Table 1 - Year 3 Main Phases

	PHASE 1	PHASE 2	PHASE 3
Duration	M24-M28	M29-M30	M31-M36
Objective	Customization of Models, Support to Toolkit development	Internal Toolkit evaluation	External Toolkit Validation
Involved users	Domain Experts Security Experts Security Training Experts HCI Experts (SoA usability standards and interface design)	Consortium Partners, Technical Partners, Domain Experts	Airport Security Stakeholders, Policy Makers: - ACI Europe - Eurocontrol - European Commission - Airports (Anadolu, Genova, Pescara, Ancona-Falconara, Esbjerg)

The following section describes the different activities carried out for the Support to Toolkit Development, ranging from the GUI Expert Evaluation and redesign, to fine-tuning data and Support to technical testing.

2. Support to Toolkit Development

The support to the Toolkit development was carried out in three phases following the process described in Figure 1:



Figure 1 - Support to Toolkit development process

2.1 Interface testing and adaptation with WP8

The GUI Expert evaluation has been carried out by Human-Computer Interaction and (HCI) and interface usability expert consortium members by applying the cognitive walkthrough and the task analysis methodology (add refs). The GUI expert evaluation has been carried out in May 2014 on the preliminary release of the tool, only for internal revision.

The expert evaluation focused on the different components of the GUI, i.e. the model selection and the launch of the scenario; the computation execution and the visualization of the results of the computation, with both a general and a detailed analysis. The evaluation also included a task analysis based on the following list of tasks that have been performed and analysed by the experts:

- Task 1_ Experts had to change Airport cost parameter
 - o 1.a: By manually insert the cost of an existing airport security measure, by using the drop-down menu.
 - o 1.b: By adding a new security measure and insert more expensive/cheaper cost than the existing ones.
- Task 2_ Experts had to change Airport measure deterrence and detection parameters
- Task 3_ Experts had to change budget parameter
- Task 4_ Experts had to change model iteration parameter
- Task 5_ Experts had to save new version of the scenario

The evaluation provided the software tool development responsables (WP8) with qualitative feedback regarding the main interface components, including a list of optimization/ remediation actions to be carried out to improve the usability of the interface and the results of the task analysis (see Appendix E).

WP1 contributed to user interaction and GUI design to tool development by also providing an overall redesign of the logical structure of the interface, see the result in Appendix F. It has been developed according to the expert evaluation described in Section 2.1.



SECONOMICS

Further input were provided to the definition of the Template to present the model results.

2.2 Tool tuning with WP5-WP6-WP8

WP1 contributed to the tool development by also defining further data and details on the Airport Security scenarios. In particular further data were collected in order to define the input parameters for two further cases included in the Security Risk Model (WP5): the case of a medium size airport in western Europe, for whose the annual financial sheet of the Turin Caselle Airport has been analysed; and the case of a big hub in western Europe, taking the London Heathrow annual financial sheet as reference.

The following table provides an example of the input parameters collected for scenario definition.

Table 2 - Input parameter for the Medium size airport in Western Europe

	2013	2012
Aeronautical Revenue (Rights, Handling, Security, Centralized infrastructures, Common goods)	36.585.000	42.115.000
Total Passengers	3.160.287	3.521.847
Average aeronautical income per passenger	11,57	11,95
Operational Costs	24.335.000	26.855.000
Security Costs (25% of operational costs)	6.083.000	6.713.000
Security Costs for the Tower (5% of operational costs)	1.216.000	1.342.000
Annual Flights number	31.866	39.664
Average low traffic	66	81
Average medium traffic	87	108
Average high traffic	108	135

2.3 Interface refinement with WP8

As for the tool internal technical testing, WP1 provided tool development responsables with the needed support for the interpretation and the harmonization of the results provided by the tool with reference to the small Eastern Europe airport, the medium size Western Europe airport and the Big European Hub.

WP1 second contribution consisted in the definition of the scenarios to be tested before the validation with external stakeholders. In particular the testing of the following cases has been requested:

- a.1 Small Eastern Europe Airport (on Anadolu Airport profile)
- a.2 Medium Western Europe Airport (on Turin profile)
- a.3 Big European Hub (on London Heathrow profile)
- a.4 AA without one countermeasure (i.e. 'x-ray' has to be deleted)
- a.5 London with the budget parameter fixed (i.e. 92.000.000 EU)

Examples of inconsistencies found during technical testing are reported below:

- results from the different cases (low, medium, high) didn't show significant differences;
- in the Big Hub scenario limited differences were noticed between the results of the low-level traffic and the high-level traffic conditions.

Those issues, and other that were identified in this activity, have been extensively discussed by WP1 and WP5 researchers and WP8 tool developers, with the goal of revising the tool and conduct further testing and finalization.

3. Support to Toolkit SECONOMICS Practice for Exploitation of Science-Based Policy Models

Our approach is a "Good Practice" on how scientific models can be introduced and used by policy makers for evidence-based policy making.

The practice in the Airport Security use case is structured according the following activities (see Figure 2):

- **Stakeholders' Buy-in:** national and EU level stakeholders were identified and engaged in the customization process from the beginning of the project.
- **Confidence building:** the needed confidence in the SECONOMICS methodology & Toolkit (models + tool) was built through presentations, training and ad-hoc analysis finalized to explore and evaluate the tool potentials in the selected domain;
- **Calibration:** data and model were calibrated on the specific requirements of the domain through data analysis, data interpretation and data inputing;
- **What-if scenario:** according to preliminary results of the analysis, the tool was tested with different input values in order to check the different outputs against the experience of the stakeholders.



Figure 2 - Activities for Exploitation of Science-Based Policy Models

The SECONOMICS research and development experts are thought to facilitate the whole process according to a role of technical consultants.

In the Airport Security case study the SECONOMICS practice has been instantiated by primarily focusing on the relevant stakeholders to involve. During the SECONOMICS project Year 3 the Airport Security case study engaged a number of organizations into the Expert Group of Airport Stakeholders, see Table 6 for the description.

Table 3 - Stakeholders involved in WP1 Year 3 research activity

Stakeholder panel member/organization	Relevant information
ENAC	Italian Civil Aviation Authority. Two units have been involved: - The Security Department, responsible for the security regulations at national level (National civil aviation Security Programme (NSP)) and security monitoring and auditing for aviation stakeholders. - The Board of Airports' Directors. The Board encompasses the ENAC Directors of the major Italian Airports and holds bimonthly meetings by discussing policy and regulatory proposals to be presented and approved by competent Authorities.
ACI - Europe	Airport Council International - European Area, Security Department Officers.
Eurocontrol	European Organisation for the Safety of Air Navigation, Security Team Representatives.
ENAV	Italian Air Navigation Service Provider, Security and Safety Departments Officers.
IATA	The International Air Transport Association (IATA) the trade association for the world's airlines, Aviation Security Training Manager.
Assoaeroporti	Italian Trade Association of the Airport Management Organisation in Italy, Security Department Manager.

4. Validation of SECONOMICS Toolkit Exploitation Practice

The European and national airport and aviation associations reported in Table 4 have been engaged into the SECONOMICS research activities by a continuous and coherent contact by mean of WP1 responsables: they were presented the overall framework of the project, the objectives and the approach; as well as the features of the airport security case study and the modeling approaches held in WP5 and WP6.

The progressive stakeholders engagement was carried out by a variety of instruments ranging from mail exchanges to voice calls; and from formal/ informal meeting to evaluation sessions on intermediate and final results of the project.

Supporting the stakeholders in being aware of the overall framework of the project represented a pre-condition to get their acquaintance and to go with them into further details of the scenarios.

The recognition of their role, competences and capability in the airport security domain allowed us to build the confidence needed to ask them to actively participate and contribute to the project, e.g. by sharing real life data and information (i.e. for calibration purposes) as well as by discussing and validating the project results (i.e. by mean of the What-if scenario).

a. Validation Activities

Stakeholder buy-in

During SECONOMICS Year 3 a plan of iterative meetings (in presence or through conference calls) with the stakeholders described in Table 4 has been scheduled.

IATA and ENAC Security Instructors, domain experts, Airport Management Organisations (such as AERDORICA), Airlines representatives and International organization have been contacted with regularity from April to December 2014 in order to involve and keep them updated about the project research results, on both technical and theoretical concepts.

Those meetings foresaw a common structure based on the general presentation about research advancements, the discussion on the project outcomes and the collection of feedback and further suggestions on how to improve the quality of the research.

At the beginning of Year 3 the above mentioned stakeholders were involved in the validation of the implementation of the models into the software tool and did appreciate a lot to see how the models became real instruments to be used by Airport Security policy-makers and decision-makers being implemented in the tool. As they have been part of the project since the use case analysis, and they provided input to scenario definition, they felt like the real owner of the Airport Security case and expected to both impact on project outcomes and being informed by research results.

Confidence building

The dissemination and validation workshop for airport security case study was performed at Anadolu University, 27-28th of February 2014 with the objectives of:

1. Sharing information about SECONOMICS project studies Airport and ATM security professionals as stakeholders,
2. Gathering the stakeholders feedback about project scenarios, models and outputs.

AU involved Turkish and South Eastern European professionals about airport security in two main activities:

- Presentation and discussion of the general SECONOMICS project and WP1 and WP4 studies presentations related to security perception,
- Focused presentations of WP1 scenarios and models on airport security and discussions.

The workshop participants were mainly from Turkish civil aviation environment who are professionals from European Commission, Turkish CAA-DGCA (Directorate of General Civil Aviation), Turkish ANSP-DHMI (General Directorate Of State Airports Authority), Airlines, Sabiha Gokcen (Istanbul) airport, Air Traffic Controller's Association (TATCA), researchers and project experts from AU.

Project partners, guest speakers and DGCA airport security representative performed the workshop presentations.

Bringing together participants and representatives of privileged stakeholders in the aviation/airport security, this highly interactive event enhanced the collaboration between researchers and practitioners.

The workshop was conceived as interactive and participatory: the organizers offered a variety of formats in which stakeholders knowledge and experiences have been shared.

Calibration

The calibration phase involved mainly the airport security domain experts in a Pre-analysis activity held in March/April 2014. In particular Experts from both aviation and IT security domains have been involved in analysing the tool through the expert judge.

In particular the following two specialists have evaluated the tool from their specific domain perspective:

- one security instructor certified by IATA,
- one former air traffic controller and aviation expert,

The expert judges identified a list of potential and existing problems and provided recommendations for how to develop the tool further. Expert analysis revealed insights and concerns currently not covered by the tool. At this stage, the purpose of the analysis was to discover and address critical problems on the conceptual level in order to provide input for fine-tuning and calibration of the tool.

In addition to the above-mentioned methodologies, semi-structured interviews have been administered with the aim of collecting relevant comments and observations from the stakeholders involved in the airport domain. Through semi-structured interviews to experts at national and international levels involved in the Falconara airport workshop and in the Final Summit, the tool scope and functionalities have been better calibrated.

In particular, the following issues were recognized as the key factors needed to be integrated into the tool:

- the human factor and the aspects of education, awareness, training and exercises as a very important package required to implement the security framework;
- the public, and its need to be aware of security issues, to be reassured, to have a general understanding of why security is taking place so that they are happy to comply with it;
- the differences among small and big airports, in proper dimensions and cultural differences.

What-if scenario

The What-If scenario sessions were made possible by the adoption of the most mature and final version of the tool that, after the iterative refinements occurred during Year 3, was ready to be evaluated through end users validation sessions. Relevant criteria examined here are:

- How users progress without strong guidance;
- How users take advantage of tool functionality in order to carry out the activities in a new, more effective way;
- Users' rating of the system in terms of group awareness, social presence and immersion;
- User's acceptance of various validation scenarios in terms of the time devoted, the extent of the collaboration and percentage of task completion and time needed;



SECONOMICS

The evaluation took place using data collecting techniques which included: group discussion, task walkthrough with application of the think aloud protocol, questionnaires with open/closed questions, interviews and debriefings and audiovisual recordings.

The Airport Security case study included three What-If scenario sessions:

- a. Demo with Application - November 2014 - Policy Makers
- b. What-if Scenarios November 2014 with Decision Makers
- c. What-if Scenarios December 2014 with Decision Makers

a. Demo with Application - November 2014 - Policy Makers

On the 4th of November the Demo with Application session took place in Bruxelles. Airport Security experts from industry (HP Security Labs), European Commission (DG Move) and international organization (IATA) have been involved in the SECONOMICS Policy Toolkit Validation with Aviation Security Stakeholders.

The following table describes the activities carried out during the session:

Table 4 - SECONOMICS Policy Toolkit Validation with Aviation Security Stakeholders

<i>Slot</i>	<i>Description</i>
Introduction	
Tool & Scenarios Demonstration	Security Risk Models (WP5) Modeling approach Economics & System Models (WP6) Modeling approach Security & Society (WP4) Scientific Approach SECONOMICS Toolkit Demo
Security Risk Models Toolkit Exercise	Live Exercise using WP5 models in the SECONOMICS Toolkit
Economic & Systems Models Toolkit Exercise	Live Exercise using WP6 models in the SECONOMICS Toolkit
Final Evaluation	Summative evaluation + Questionnaire

b. What-if Scenarios November 2014 with Decision Makers

The SECONOMICS Tool Anadolu validation workshop was performed at Anadolu University Airport at 21st of November 2014. The workshop consisted of two sessions:

1. General SECONOMICS studies and Tool presentation,
2. Focused interaction with Tool and participants.

The validation workshop objectives can be presented as:

3. Sharing information about SECONOMICS project studies with the stakeholders who are high level professionals about Airport and ATM security,
4. Having the stakeholders ideas about project tool scenarios, models and outputs by discussing on the provided data of WPs.

Anadolu University involved the Anadolu airport managerial and operational personnel and professionals about airport security in order to let them contribute to the SECONOMICS Toolkit studies by their high-level knowledge and experiences



SECONOMICS

as stakeholders. The workshop participants are Airport Accountable Manager, expert air traffic controller, airport security expert and instructor and former CNS/ATM Safety Manager.

c. What-if Scenarios December 2014 with Decision Makers

On the 1st of December 2014, the Tool Validation Workshop held in Ancona-Falconara Airport involved the Management and Security Board of three different Central Italy medium size airports, i.e. Ancona-Falconara Airport, Perugia Airport, Rimini Airport). These stakeholders have been involved in the project since the scenario preparation and fine-tuning through a series of conference calls and two workshops at the Anadolu University Airport and at the Ancona-Falconara Airport, as reported in Deliverable D1.4 “Model Validation”. Alongthrough Y1 and Y2 activities such institutions were engaged in Stakeholders buy-in and Confidence building about project methodology and approach and were particularly interested in getting updated about the advancements and the outcomes of the research.

Within the broader scope of evaluating the potentials of the SECONOMICS outputs towards the functional and security requirements featuring the airport security decision-making, the specific objectives of the Workshop were:

- To present the final results to airport security stakeholders,
- To discuss and validate the tool for airport security decision making by mean of ‘what-if’ scenarios implementation.

Together with Falconara Airport personnel, partners from DBL and UNITN participated into the event as airport security case study responsible.

A total of 5 people from the Airport operation management were involved in the Worskhop activities: the Aerdorica Security Manager, the ENAV Ancona-Falconara Tower responsible, the Rimini Airport security manager and technical officer, the Perugia Airport security manager.

During both the Falconara and the Anadolu Workshops, the following activities have been carried out:

- Focus groups dedicated to tool walkthrough, during which the tool features have been presented and discussed,
- Live exercises to let participant directly interact with the tool by customizing and simulating selected Airport Security scenarios (see the protocol below for further details).

Both the activities involved the participants in step-by-step evaluation of the SECONOMICS Toolkit. This allowed to assess the proposed methodologies and to identify potentials and weaknesses. These activites were structured according to the following protocol:

1. Tool demo

The users got introduced with GUI components, main functionalities and stages

2. Familiarization

The users familiarized with the SECONOMICS tool. Through the completion of this session they were capable of answering a

questionnaire regarding issues such as usability, user experience, appearance, aesthetics, interactivity and adaptability and activities to be performed on the tool.

3. Live exercises

The users were involved in Live Exercises, trials that allowed them to explore and appreciate the potentials of the tool and to have a direct experience of use of the tool and be capable to validate it by:

- a. Varying the input parameter to the tool (input costs, input security measure, detection/ deterrence level)
- b. Building their own scenario

Step a. included the following schema:

Task 1_ Load one case by selecting among the three available ones

Task 2_ Change Airport cost parameter in one previously selected case of the scenario

- 2.a: Manually insert the cost of an existing airport security measure, by using the drop-down menu.
- 2.b: Add a new security measure and insert more expensive/ cheaper cost than the existing ones.

Task 3_ Change Airport measure deterrence and detection parameters

Task 4_ Change budget parameter

Task 5_ Change model iteration parameter

Task 6_ Save new version of the scenario

The following Validation instruments have been administered to participants in order to collect their feedback:

- the Evaluation Questionnaire for the SECONOMICS Tool, for which the System Usability Scale (SUS) has been used and adapted. SUS is a simple, ten-item attitude Likert scale giving a global view of subjective assessments of usability (Brooke 1996). Such an instrument provided us with data related to Technical Usability (see Annex 1);
- the Final Evaluation on SECONOMICS results, a six-item attitude Likert scale comprising the models, the models' results and the tool (see Annex 2);
- the Validation Support Questionnaire, a Likert scale questionnaire investigating Domain Suitability and Future development of the SECONOMICS Tool (see Annex 3);
- the SWOT-alike form, comprising strengths, weaknesses, suggestions and concerns about the SECONOMICS tool (see Annex 4);

b. Validation Results

User Acceptability

Strengths related to tool implementation and user acceptance

- The Final Evaluation on the SECONOMICS results proved a general acceptance and appreciation of the mechanisms and computational strategies under the models; the models' results quality and usefulness; and the tool implementation and effectiveness. Models coverage and models' results visualization have been of great value for the workshops participants.
- Stakeholders involved in the Anadolu and Ancona-Falconara airports workshops rated the SECONOMICS tool as valuable for analyzing different security-critical scenarios and forecasting the impact of the different security measures within the selected case.
- Stakeholders involved in the Anadolu workshop found the tool flexible depending on the different countermeasures. The tool provides an easy input selection layout and also gives a vision for the user.
- The Toolkit has been appreciated and fully accepted by the stakeholders involved in the final validation session. Policy-makers in the airport security domain evaluated the Toolkit as an integrated set of instruments with its own internal coherence and effectiveness. The users were satisfied with the functionalities and the opportunities the Toolkit offers.

Issues requiring improvement and enhancement

- Input parameters (i.e. equipment costs and wages, as well as security budget) need to be further revised since each cultural and national context needs suitable and realistic data.
- The tool requires theoretical background for the security parameters and calculation of the tool. Reporting graphics were found insufficient and iterative modeling error history is not given.
- Respondants to the Validation Support Questionnaire reported that the tool is considered effective to improve the process of decision making by reducing the complexity of this process in Airport Security and increasing user security-specific knowledge although using the tool would probably require more effort than using standard decision-making techniques.
- On the other hand, the involved stakeholders considered the support of a technical person needed to be able to effectively use the tool since it has been considered complex, especially because it is not required to be learnt by users as daily usage tools do.

Domain Suitability

Strengths related to tool suitability for the Airport Security domain

- The Toolkit was evaluated as suitable for the Airport Security domain since it recognizably covers all the needed information and concepts required by such a domain. By mean of the involvement of a wide variety of professionals and expert, the knowledge represented in the Toolkit has been made consistent and valid.
- During the What-If session at the Anadolu Airport workshop the participants were highly involved into all the sessions and contributed by asking

questions and discussions also performing the tool interaction. The scenarios and modeling about airport security were found meaningful considering ATM operations in the center of all airport operations.

- Policy-makers in the airport domain considered the Toolkit as a valuable instrument for supporting the airport management companies in tackling possible conflicting goals: on one hand they need to minimize costs and maximize security investments, on the other they must guarantee security standards according to EU and national regulations. Such a contextual knowledge should be integrated into the Toolkit, especially when describing the policy guidelines.

Suggestions for enhancing the scenario and issues requiring improvement

- Along through the different validation sessions, the stakeholders repeatedly asked for further refinement of the data provided in the input table. Their request was related to validate if and how the model could be generalized and could address heterogeneous needs coming from different airports.
- During the What-If session at the Ancona-Falconara Airport workshop, the involved stakeholders suggested to investigate an actual real-world Airport Security case: the internal airport security service gate management. Service gates are both used for personnel and transport means movement. Until few weeks ago the police have been in charge of managing the internal service gates through which officers and allowed personnel may move from the different areas into the airport. Such a responsibility has been recently assigned to the Airport Management company security responsables. This change may affect human resources:
 - selection process and criteria
 - training process
 - enrolement.

The service gate case is thought to be of interest for investigation and deployment under the SECONOMICS framework.

- The following improvements of the tool have been pointed out:
 - need to consider the shift and the impact of class contract
 - need to differentiate machine buy-in from maintenance contract
 - need to verify personnel roles incompatibility
- The security and risk profile of the actors are expected to change along time and to be shown, together with the optimal security investment strategy.
- The tool should better address the effect of familiarization of passengers with the different security measures (e.g. x-ray device Vs 3D body scanner): more the security measure are familiar, more easily the passenger could accept their adotion.
- It would be highly appreciated the opportunity to extend the tool adoption from individual airports to networks/ clusters of airports.

Technical Usability

Strengths related to tool usability



SECONOMICS

- The Validation sessions at the Ancona-Falconara and Anadolu Airports involved the users in direct interaction sessions with the tool and with the models behind. The Toolkit was firstly presented within the SECONOMICS framework and outcomes and then proposed to the users for autonomous exploration and guided task execution. Both the Familiarization and the Live exercises with the tool involved about ten people from policy and decision making in direct use session. The participants were highly involved into all the sessions and evaluated the GUI look and feel and memorability of great value. The Toolkit provides an easy input selection layout and a comprehensive overview of the scenario, which allow the user to understand the results.
- From System Usability Scale Questionnaire (SUS):
 - the majority of respondents proved a general satisfaction with using the tool. Its functionalities and components were evaluated interesting and exhaustive.
 - the tool was considered easy-to-use without the support of external consultants.
- The Validation Support Questionnaire results also showed that the model is easy to learn/recall from memory.

Suggestions for enhancing the tool

- Stakeholders suggested that the integration with Excel dataset would improve the effectiveness and suitability of the tool.

5. Policy Insights from Validation

5.a) Summary of Findings at the Validation

In this section we present a summary of the policy findings that have come out of validation meetings/workshops. The understanding and knowledge of policy in the area of Airport Security that have been gained is much wider than what can be put in this section.

Summary findings:

- Stakeholders involved in the validation process and listed in table 3 agreed that Cybersecurity is becoming more and more relevant issue in Airport security. Nowadays security financing has used diverse instruments such as government subsidies or security taxes depending on size and passengers. A popular scheme is a flat security tax per passenger of 5-7 Eu in Europe and \$5.6 in the USA. A key question for regulators at EU level is whether the same regulatory and financial measures should apply to cyber-security. Due to the tightly interconnected nature of IT systems, SECONOMICS results highlighted how interdependency issues impacting the probability of a successful attack can make regulation significantly unfair for small or medium airport. This finding has been considered as a valuable input to make current regulation evolve. For the scientific policy paper please see *WP6 D6.4 Compendium Annex Policy Paper 5* for the scientific summary
- The prescriptive and static nature of the current normative corpus is strongly criticized mainly by airport managers interviewed in favour of a more risk-based approach, that should consider additional plug-ins to the normal baseline regulation (i.e., minimum required security provision) fitting the specificities of different airports. The preference accorded by the Airport Security stakeholders to a risk-based approach is supported by the need of a contextual, shared and complete risk assessment to be done in collaboration with international regulator bodies and national aviation authorities. The regulation should be based on the real risk, in order to deliver effective security outcomes, a direction toward which the European regulators are trying to move (for more details see the Policy paper in Appendix G).
- All the stakeholders involved in the SECONOMICS activities confirmed the value of the human factor in making the security training policy evolve to a more effective stage. Airport security regulations are constantly evolving, thus the need for staff to be fully trained to ensure security of an airport is of vital importance. Moreover, today's radical changes in the forms of security threats require exerting even more effort to develop the desired knowledge, skills and attitudes in work-force. Employee training to keep up with new trends and practices therefore has generally been considered as a crucial factor for airport security management (ASM). As stated during SECONOMICS validation activities by airport security experts and security managers, security training for airport personnel is widely recognized as a very important activity for guaranteeing airport security and can be a

powerful facilitator of enhancing airport security. However, the efficacy of security training programs in enhancing the security attitude and the capabilities of employees cannot be taken for granted. For the scientific policy paper please see *WP6 D6.4 Compendium Annex Policy Paper 3* for a detailed summary.

- The Validation of the Security and society model (WP4) included the evaluation on social acceptance and highlighted relevant issues for policy makers and national/regional governments about communication to the general public/citizenship. Technologies, viewed as intrusive towards the private or intimate spheres of individuals, receive a more negative coverage even if the particular security risk is perceived as high (especially 3D body scanner). Health, privacy and dignity concerns prevail over security risks (whose probability is seen as low). The media is shifting from a focus on security threats to an awareness of the possible trade-offs of security measures in terms of health, privacy, freedom, and civil liberties. The public is becoming more sensitive not only to threats but also to the costs of security and media play key role in shaping political communication and public attitudes - informative and educational functions, and increasingly provide platform for public political discourse, including provision of space for the expression of dissent. For more details see *D4.5 Comparative analysis of public attitudes to security and acceptance of risk*.

5.b) Summary of findings at the Summit Conference

At the SECONOMICS Summit a designated panel was scheduled focussed solely on the Airport workstream with the aim being to contextualise and discuss main trends and problems in Aviation Security regulation.

The session consisted of presentations from 4 different Invited Speakers followed by a Question - Answer Discussion session with all speakers as panellists. This panel session aimed to link the SECONOMICS research themes to the needs and perspectives of the European stakeholders in the Aviation domain.

The organisation of the panel is described in the following table:

Table 5 - Organisation of the Airport Panel at SECONOMICS SUMMIT

11.00 - 11.15	Darren Handley DG Move Aviation Security	How do Socio-economic issues affect Aviation Security Policies and the future of Aviation Security?
11.15 - 11.30	Antonio Nogueras Eurocontrol (BE)	Emergent challenges and opportunities in ATM Security focusing on increasing automation and cyber-security.
11.30 - 11.45	Eli Mandelawy IATA (CH)	Security Training and Awareness Raising in the Aviation domain.
11.45 - 12.00	Marc Sel Pricewaterhouse and Cooper - Belgium (BE)	How Aviation Security can benefit from policies, standards and best practices in other domains.
12.00 -	All	Q&A - Plenary Discussion



SECONOMICS

12.30

Table 5: SECONOMICS Aviation Security Panel at the Final Summit.

Main findings during the Airport Security Panel were reported below:

- Aviation Security requires a holistic approach including investigation of all the interfaces between aviation security components e.g. ATM security, CNS Security, Airspace Security and Airport Security. EU needs to address the variety of threats and challenges to aviation, including:
 - all phases of air transport;
 - on the ground and in the air;
 - all operational processes related to the Airport , the Aircraft and Air Traffic Management;
 - passenger awareness as part of the process;
 - the importance of international relations and the need for working with/through wider regional/international organisations such as ICAO/ECAC/EUROCONTROL as well as with industry stakeholders;

On such a premise the stakeholders involved in SECONOMICS agreed on recognizing the need to improve resilience of the whole air transport system as well as to assess public perception and acceptability to risk and security rules and to better define current and future vulnerabilities. The Security Risk Models (WP5), the Economics & System Models (WP6) and the Security & Society (WP4) model are considered

- The EU regulator needs to address the needs of approximately 660 airports in the EU. Only ten are probably very innovative and try to look at things differently, investing in new technologies and new processes to improve security and processes. Many airports tend to invest their scarce resources where they can get the best return. Hence many do not invest in security until changes in regulation force them to or circumstances make it beneficial for them to (for example equipment comes to the end of its life). In this context the SECONOMICS Toolkit may impact on socio-economic issue of security management.
- All stakeholders participating to the SECONOMICS Final Summit agreed on the SECONOMICS modelling choice to decompose the cross section of EU airports into size categories and on the relevance of this grouping for the characterization of different needs and security requirements. It was also highlighted the fact that small and large airports do have lobbying groups at EU and worldwide level that are divided by airport size.
- Airport security management also includes the knowledge of the different national taxation systems. The Commission merely specifies that airport security costs can be recouped, without specifying how (see art.5, EC300). It varies from member States, even areas or airports. For example in Germany there is a general tax that funds the state operators. In Italy passengers pay by person. There is no uniformity about security charges and they can cover different things: sometimes they just cover equipment; sometimes they cover equipment and some of the staff; sometimes equipment and all of the staff, even staff that is not directly involved in security.

5.c) European Coordination

During the whole SECONOMICS project WP1 actively involved airport security stakeholders and high-level policy makers in the validation process to assess SECONOMICS outcome and properly customise them for the Airport domain. Representative members of the main EU Institutions and Organisations in the Aviation domain were engaged to ensure proper coordination at trans-national level and compliance with current regulations and future trends. Main interesting issues that need a ‘pan-European’ approach were the following:

- SECONOMICS WP6 models have demonstrated that fair cost sharing across the European aviation sector is not trivially implemented. Large airports have economies of scale and one passenger taxation model will, in all likelihood, result in unequal cost sharing, in some form or another. Our models indicate that attacker elasticities further complicate the fair cost sharing arrangements and this concept was broadly agreed by the European stakeholders involved in validation activities and participants at the summit.
- Due to the international and trans-sectorial nature of the cyber threat itself, a more transborder, trans-sectorial and collaborative security regulation would be required. The problem here is the lack of a global framework for cyber security in aviation. We need to address cyber security in aviation in a more holistic way, meaning all security actors and all aviation players have to be encompassed under the same framework. The regulation has to consider all these aspects, whilst ICAO reported that five major international aviation organizations signed a roadmap towards aviation cybersecurity agreement only in Dec. 2014.

6. Future and Emergent Threats

According to data collected at the Final Summit Conference through structured interviews with policy makers, the tool needs to be improved with the enhancement of the future and emergent threats scenario. The background and contextual information, as well as the new and emergent attacks and the need for regulation, ought to be integrated in the scenarios the tool implements.

Changing Regulation

The overarching regulation in Aviation Security (EC300/2008), and, within that, the Regulation 185/2010 and Decision 774/2010, define the EU baseline which encompasses elements of risk management. In formulating the regulation the EC identifies the risks and what can be done about them. There may be also some risks where we cannot do anything about, for example they may be too difficult to mitigate without hindering the flow of traffic. Where it is unfeasible to implement a mitigation, risk is managed.

This is the case of new and emerging threats, for which regular committees and working groups meet on regular basis and review the threat situation with the Member States. Intelligent services from member states tell the Commission what

the latest threats are. Member States sometimes come directly to the Commission to inform her about threats, leading us to review the baseline and if we think there is an urgent need to move it, we will go through an urgency procedure, which is exactly what it is, a speeding up the procedure to put the new regulation in. Alternatively the ordinary procedure is adopted, which takes a bit longer, but is essentially the same and amends the regulation.

Hiding Explosives

The threats currently under major expansion regards new ways of hiding explosives, i.e. new vectors to try to get the explosives in the airport. Attackers try to hide explosives in their shoes, their underpants, in cargo. There are a lot of different ways of hiding the explosives and the method used by terrorists will continue to change. At the same time, the EC cannot easy to say what the emerging risks are and what their consequences may be.

Cyberthreats

EU Policy makers in the Airport Security domain stated that the lack of a global framework for cyber security in aviation is still pending. In the EU context cyber security needs to be tackled in a more holistic way, meaning all security actors and all aviation players have to be encompassed under the same framework.

There is also a need to link the aviation sector with other sectors, like the airport security, there is a clear interdependency between sectors. The attackers do not care about which sector they are attacking, the only thing they care about is the benefits they can get from it. The same for the borders: attackers are multinational and cross-border. The regulation has to consider all these aspects and the tool has to elaborate the scenarios into usable and structured knowledge.

7. Conclusions

The WP1 Tool validation process described in this deliverable allowed us to evaluate the UI implementation approach, the scenarios, the models themselves and the results in a comprehensive and integrated way. The validation has been made possible by the application of a methodology defined ad-hoc for the validation of models and modeling approach, integrating state-of-the-art validation methods.

The validation process for the Airport Security, both including the policy guidelines and the software Toolkit showed general acceptance and appreciation of the mechanisms and computational strategies under the models and of the models' results quality and usefulness. The tool implementation effectiveness has been also validated from both decision-making and policy-making stakeholders. In particular they evaluated the Toolkit as an integrated set of instruments with its own internal coherence and effectiveness, ready to be customized on the basis of requirements from the field and be applied in specific cases.



References

[1] de Gramatica, M., Massacci, F., Shim, W., Turhan, U., Williams, J. (2014) "Agency Problems and Airport Security: Quantitative and Qualitative Evidence on the Impact of Security Training".

Annexes

Annex 1 - Evaluation Questionnaire for the SECONOMICS Tool Template

System Usability Scale	How much do you agree or disagree with the sentence?				
	Strongly agree	Rather agree	Difficult to say	Rather disagree	Strongly disagree
I think that I would like to use this tool frequently.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I found the tool unnecessarily complex.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I thought the tool was easy to use.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I think that I would need the support of a technical person to be able to use this tool.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I found the various functions in this tool were well integrated.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I thought there was too much inconsistency in this tool.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I would imagine that most people would learn to use this tool very quickly.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I found the tool very cumbersome to use.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I felt very confident using the tool.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I needed to learn a lot of things before I could get going with this tool.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



SECONOMICS

Annex 2 - Final Evaluation on SECONOMICS Results Template

	How much do you agree or disagree with the sentence?				
	Strongly disagree				Strongly agree
	1	2	3	4	5
a. The SECONOMICS models are comprehensible and easy-to-understand.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
b. The SECONOMICS models assure the appropriate coverage of the socio-economic security issues implied.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
c. The SECONOMICS models assure the appropriate completeness of the needed knowledge and information.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
d. The SECONOMICS models' results seem useful in my perspective.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
e. The SECONOMICS models' results are effective in supporting socio-economic security decision.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
f. The SECONOMICS models' results are effectively represented and easy-to-understand.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



Annex 3 - Evaluation Questionnaire for the SECONOMICS Toolkit Template

Instructions for using this questionnaire (please read carefully):

- 1) Before starting filling the questionnaire, please read through the questions to get a rough overview about the criteria.
- 2) The questionnaire has two scales for each criterion (statement): Please indicate for each criterion on the left scale whether the criterion is fulfilled. And indicate on the right scale how important this criterion is to you in general. On page 6, you can note identified problems issues with the model
- 3) You will fill in the questionnaire after the end of the session.
- 5) After completing the questionnaire, please return it to us.

Thank you!

Criteria for the SECONOMICS Tool	Is the criterion fulfilled?				
	Strongly agree	Rather agree	Difficult to say	Rather disagree	Strongly disagree
Domain Applicability					
The SECONOMICS Tool can be used by consultant to model and analyse the case study in support of the policy-makers.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
If consultants create models with SECONOMICS Tool, the models and the results can be understood by policy-makers.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The SECONOMICS Tool can be used by policy-makers , at least partially , to model and analyse the case study.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The SECONOMICS Tool can be used by policy-makers , in complete independence , to model and analyse the case study.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
No additional knowledge or research is required to run the SECONOMICS Tool.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The SECONOMICS Tool can be used in the existing case study processes/ workpractice.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The SECONOMICS Tool can be used without major revision of the existing processes/ workpractice.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



SECONOMICS

The SECONOMICS Tool contributes to a better support for security management in the aviation domain

Future development of the SECONOMICS Tool

1. Would you be interested in additional functionalities? If so, please specify which ones.

2. Would you need further data / outcomes to support decision making? If so, please specify which ones.

3. Would you be interested in different results' visualization modalities? If so, please describe by also sketching the kind of visualization that you have in mind.



4. Would you be interested in tool interoperability with existing software? If so, which software and for pursuing which purposes?

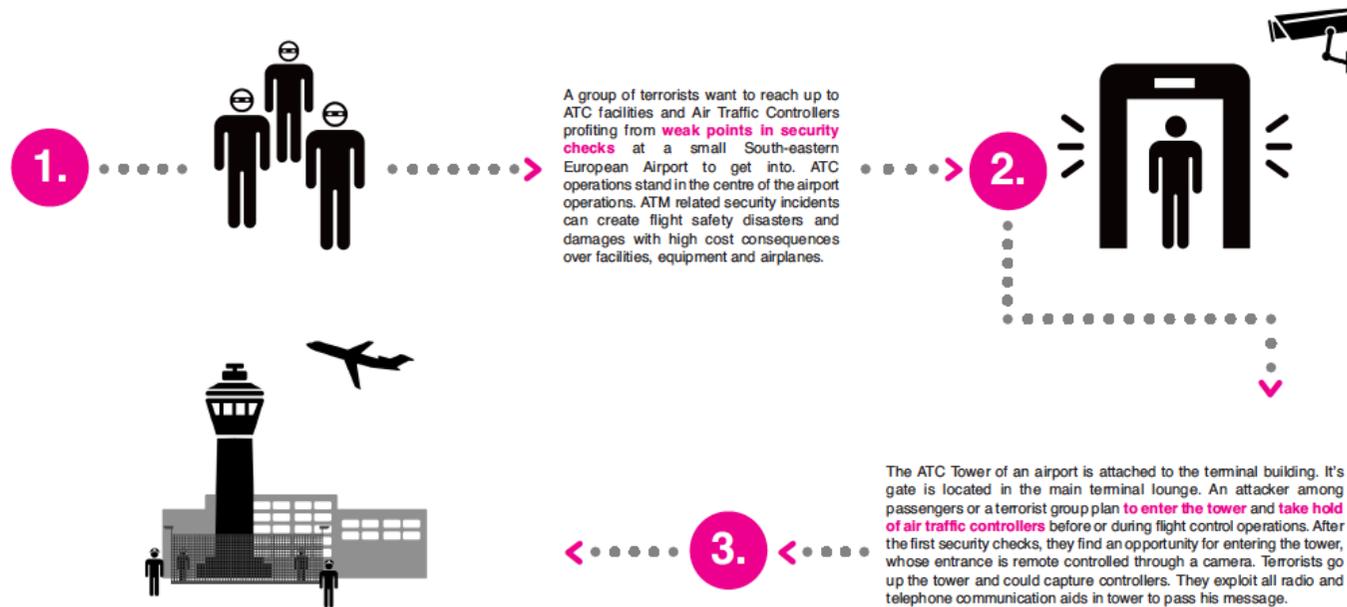
5. Would you be interested in the possibility to automatically get results' report? If so, which kind of outcome would you prefer?

Annex 4 - Airport Security Infographics

WP5 - Security Risk Model

SECONOMICS - SCENARIO

Attack to the tower



The attack may entail a major crisis for air traffic operations in the air field and airspace. **Flight safety will be negatively affected** and air traffic should be diverted to other ATC unit or airfield. All flight operations are **cancelled or diverted** to alternative airfields. Besides the safety and security impacts, the cancellation costs can be enormous possibly affecting connected national and international flights and/or airports/airspaces. Media will likely inform people immediately about the situation. This will cause new emergencies around the airport facilities and operators. Moreover, the situation will lead to a **negative security perception for airport** users and could cause a decrease of air traffic in the short-term.

SECONOMICS - MODEL
Attack to tower

The **Adversarial Risk Analysis** model has been adopted to provide airport authorities with the optimum portfolio of preventive measures in the scenario.

The **defender** formulates strategies based on compliance with policy and regulation and with what she know about hackers to deter them from attacking her IT infrastructures.

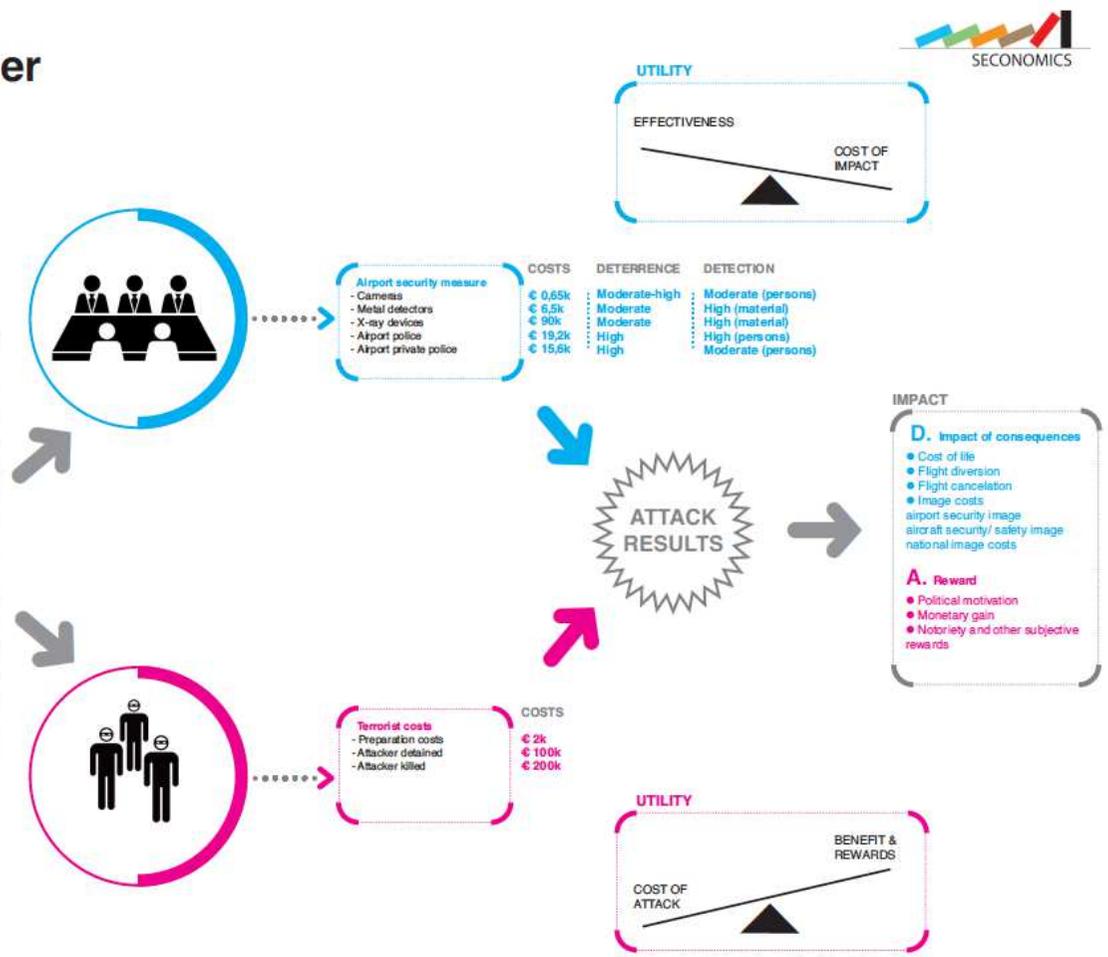
The **attacker** faces uncertain situations and needs to make a choice from a set of available actions each having different probability of yielding an outcome.

The **uncertainty** associated with the success of an attack is probabilistically dependent on the actions of both the Attacker and the Defender.

The computation proceeds through the following high-level steps:

1. Solve the **Defender's** problem optimising the defensive measures adopted with respect to potential attacks.
2. Solve the **Attacker's** problem to obtain a probability distribution that gives us information about the attack that will be chosen given the possible defensive measures that the Defender could eventually deploy.

The final output of the model will be to provide advice to airport authorities for devising an optimal security plan with the portfolio of defensive measures that will maximize the Defender's expected utility.





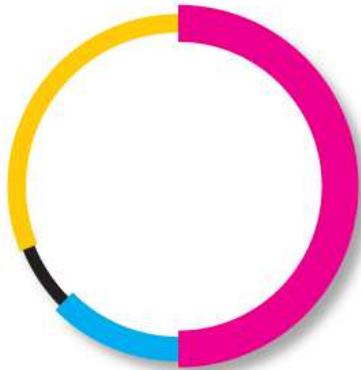
SECONOMICS - OPTIMAL INVESTMENT PORTFOLIO

Attack to tower

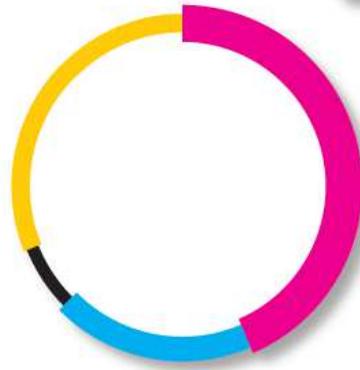
We consider the case of a small-size international airport, with less than ten connections per day. It has an average annual budget of 3 million euros, with around 5% of the total budget, 150,000 euros, to be invested on new security measures.



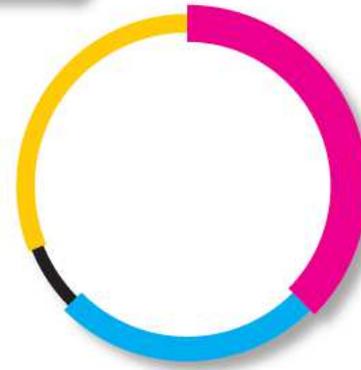
- Airport police
- Cameras
- Metal detectors
- Security guards



1. Low-traffic level airport
 In this case the airport has one international flight and four training local simultaneously.
 The optimal portfolio for the Defender corresponds to $x = (4, 1, 0, 5, 1)$, with an **associated total investment of 120,700 euros** distributed as (2600, 6500, 0, 96000, 15600) between the five countermeasures. This portfolio has considerable associated costs (but always below the maximum budget available). By deploying it airport authorities minimise the risks and consequences of terrorist actions, devising a security and cost-effective security plan.



2. Medium-traffic level airport
 In this case the airport has two international flights, one domestic flight and six training local flights simultaneously.
 The optimal portfolio was (4; 1; 0; 5; 2), corresponding to 4 cameras, 1 metal detector, 5 policemen and 2 security guards. It has an associated **investment of 136,300 euros**.
 By entailing a moderate investment, **this portfolio assures to protect the airport in the best manner** throughout the different traffic conditions, i.e. low-traffic, medium-traffic and high-traffic levels.

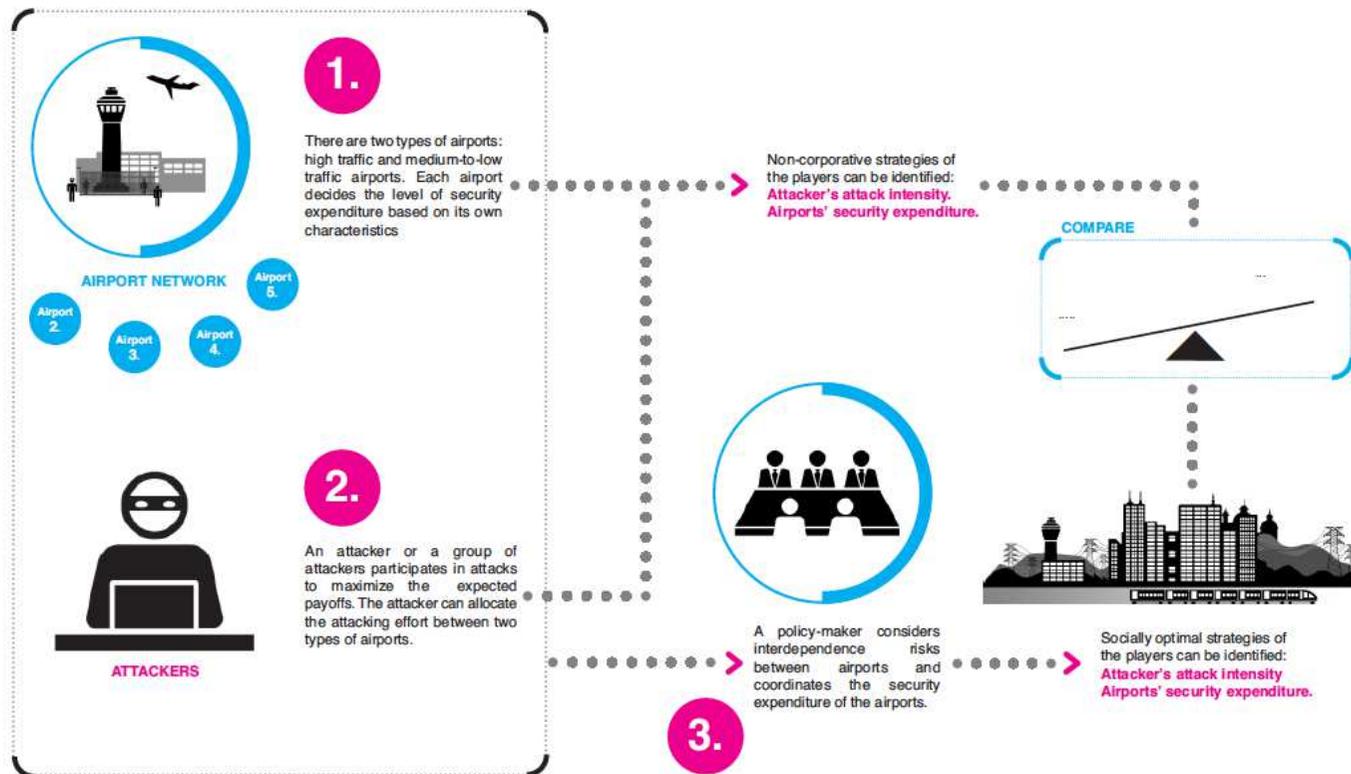


3. High-traffic level airport
 In this case the airport has four international flights, two domestic flights and eight training local flights simultaneously.
 For the high traffic level scenario, the optimal portfolio was (4; 1; 0; 4; 4), corresponding to 4 cameras, 1 metal detector, 4 policemen and 4 security guards.
 It has an associated **investment of 148,300 euros**. As we can observe, under this new scenario of higher expected losses, the operator would opt for a more expensive portfolio, exhausting almost entirely the available budget.

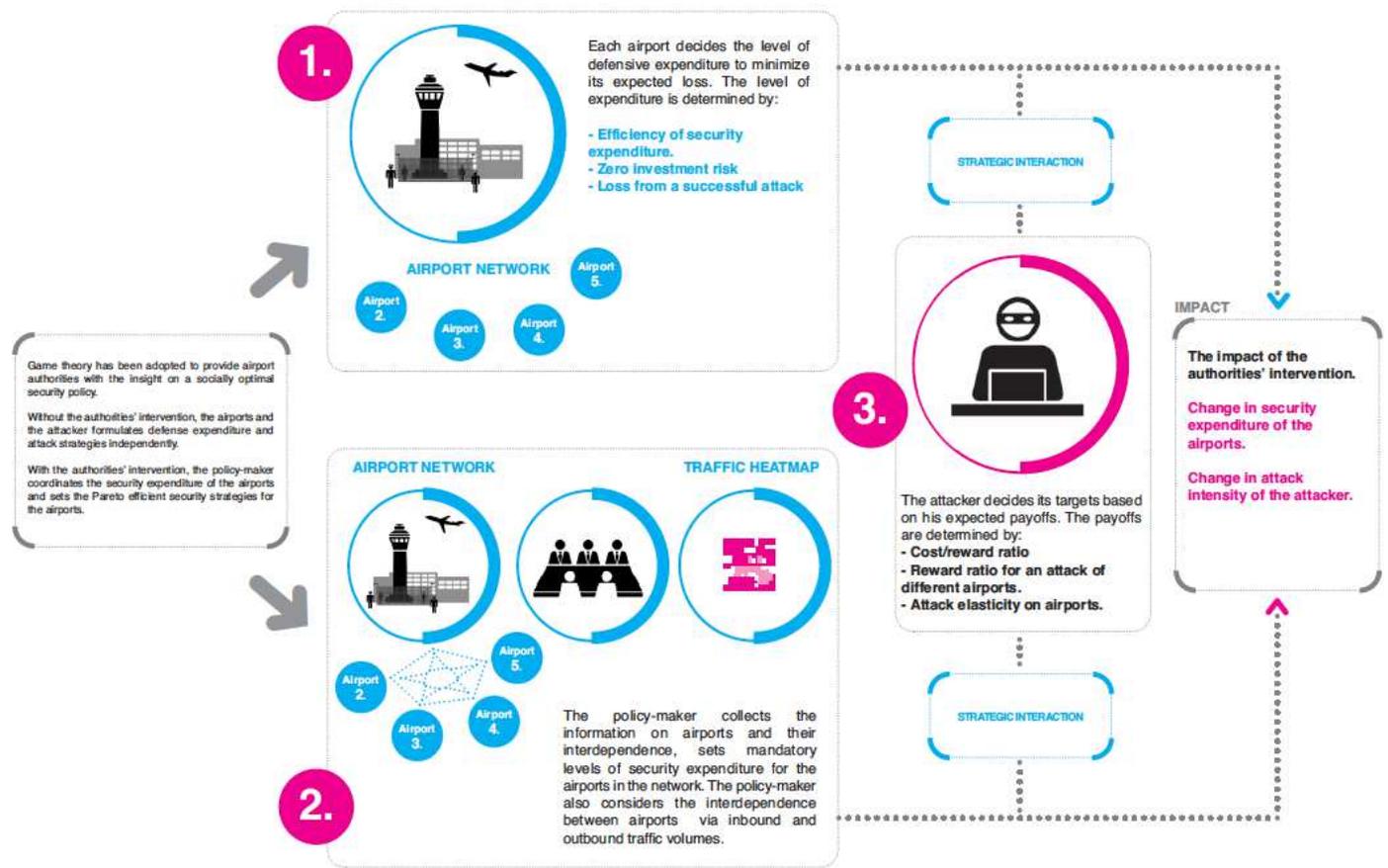


SECONOMICS - SCENARIO

Effective Security Policy Scenario



Effective Security Policy Model



SECONOMICS - OPTIMAL INVESTMENT PORTFOLIO

Effective Security Policy Model

The model considers the effects of the interaction of a policy-maker, airports and an attacker, and how best a policy maker can design an airport security policy to jointly distribute the relative cost of security investments among airports. The model has taken into account two profiles of airports: (1) high traffic airports, and (2) medium to low traffic airports

Value Assumptions

High traffic level airport

- Marginal reduction in the probability of successful attack for additional €1000 spent in security: 0.02%
- Zero investment risk: 100%
- Loss from a successful attack: 100M Euro

Medium-low traffic level airport

- Marginal reduction in the probability of successful attack for additional € 1000 spent in security: 0.02%
- Zero investment risk: 70%
- Loss from a successful attack: 10M Euro

Attacker

- Relative increase in probability of successful attack for additional €1000 spent in attack: 0.05%
- Reward ratio for high to medium-low airports: 0.7
- Cost/reward ratio: 0.1

Policy-maker

- Weight of high traffic level airport: 1
- Weight of medium-low traffic level airport: 0.8

Environment

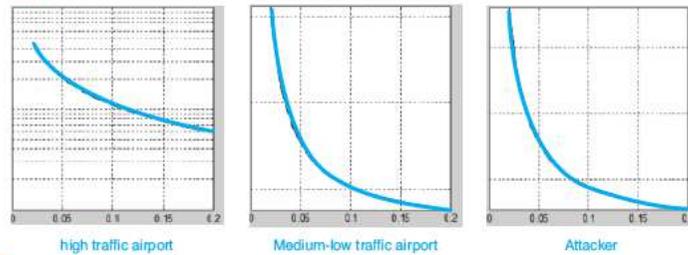
- Fraction of high traffic level airport: 0.1
- Interdependence calculated from traffic heatmap

Illustrative results:

Effect of change in a high traffic airport's marginal reduction in risk on security expenditure and attack intensity

Non-cooperative Policy:

A level of security expenditure is a chosen level by each airport attempting to minimize its own expected loss.



Cooperative Policy:

A level of security is a chosen level by a policy maker to drive the airports towards the optimal expenditure on security for minimizing total expected loss.





Annex 5 - SWOT analysis about the SECONOMICS tool template

Please indicate below which issues do you consider as strengths or weaknesses about applicability and efficacy of the SECONOMICS tool for the selected domains.	
STRENGTHS	WEAKNESSES

Please indicate below any things you would like to suggest for future exploitation of the SECONOMICS project results and any concerns you have about the suitability of the tool to support socio-economic security decision making.	
SUGGESTIONS	CONCERNS



APPENDICES

A. Assessment of Project KPI for the Scenario

ID	Short Name	Key Performance Indicator value	
		KPI Scale	Results
1	<i>METHODOLOGY and GUIDELINES for POLICY MAKERS</i> [Scale 1-5]		<p>3. Explicit linkage of produced artefacts There is an explicit linkage with the Security and Society models (WP4) produced from the study of security factors at AA.</p> <p>4. Formal linkage of produced artefacts There is a formal linkage of the Toolkit with Security Risk Model (WP5) and the Economics & System Model (WP6) implemented.</p> <p>5. “Local” Usability of methodology in producing artefacts The Toolkit requires to have a specific explanation on the SECONOMICS usage model in order to understand and exploit its potential within the airport security models.</p>
2	<i>MODELLING NOTATIONS and LANGUAGES for SYSTEMS DESCRIPTIONS</i> [Scale 1-5]		<p>2. Computer Aided support of consistency The Security and Society coding models (WP4) are conceived with the specific airport security data and are tool supported</p> <p>3. Formal characterization of constructs There is a clear characterization of the constructs adopted in the Security Risk Model (WP5) and the Economics & System Model (WP6) implemented.</p> <p>4. “Local” Usability of construct The construct is transparent to the user. She only requires a specific explanation on the SECONOMICS constructs in order to understand and exploit its potential within the airport security models.</p>
3	<i>ALGORITHMS and COMPUTATION for ECONOMICS and RISK ASSESSMENT</i> [Scale 1-4]		<p>3. Computer Aided Computation. There is a fully automatic or interactive implementation of Security Risk Model (WP5) and the Economics & System Model (WP6) in the Toolkit.</p> <p>4. Formal or operational <u>evidence</u> of efficiency. A full precise result of Security Risk Model (WP5) implemented is only possible after running thousands of iterations, so it is not possible to get accurate results on the fly. Operational evidence of efficiency of Economics & System Model (WP6) implemented was not experimented in a structured way.</p>
4	TOOL		<p>As for the Security Risk Model (WP5) and the Economics & System Model (WP6) the tool supports the methodology and computation so the same criteria apply to the supported artefacts. It is fully integrated with methodology.</p> <p>This indicator is not applicable to the Security and Society models (WP4).</p>



SECONOMICS

5	<p><i>EFFECTIVE USAGE</i> [Scale: Applied on the case study 1-4 Requiring Human Effort 1-3]</p>	<p>The research technique can be applied on the case study</p>
		<p>2. Results can be understood by the stakeholder Results can be understood by the stakeholder for the Security and Society (WP4) models</p> <p>3. Can be done by the stakeholder, at least partially Can be done by the stakeholder for the Security Risk Model (WP5) and the Economics & System Model (WP6)</p> <p>4. Can be done by the stakeholder, in complete independence Can be done by the stakeholder, somewhat independently for the Security Risk Model (WP5)</p>
		<p>Required human effort</p> <p>1. Doable Major changes in the Security and Society (WP4) models, Security Risk Model (WP5) and the Economics & System Model (WP6) require re-modelling effort.</p> <p>3. Saves effort Slight changes in the Security and Society (WP4) models, Security Risk Model (WP5) and the Economics & System Model (WP6) require re-modelling effort.</p>
6	<p><i>INNOVATION POTENTIAL</i> [Scale 1-4]</p>	<p>3. The technique can be used by revising the existing processes The technique can be used by revising the existing processes for the Security and Society (WP4) models, and the Security Risk Model (WP5) and the Economics & System Model (WP6) implemented.</p>
7	<p><i>CASE STUDY SPECIFIC</i> [Scale: Detail of Investigation 1-4 Facets considered in the Scenario 1-4]</p>	<p>Detail of investigation</p>
		<p>2. Empirical exercise (e.g. with students) to simulate steps Empirical exercise with students to simulate steps was accomplished with the Security and society (WP4) model with the analysis of national media for the related security aspects.</p> <p>3. Empirical exercise by stakeholders to simulate fractions of the process Empirical exercise by stakeholders to simulate fractions of the process. This was the level reached with the Economics & System Model (WP6).</p> <p>4. Empirical exercise by stakeholders to recreate whole process Empirical exercise by stakeholders for whole process. This was the level reached with the Security Risk Model (WP5).</p>
		<p>Facets considered in the scenario</p>



SECONOMICS

		<p>3. Multiple views (WP techniques) to a single aspect Multiple views to a single aspect has been considered in the Security and Society (WP4) models and Security Risk Model (WP5) and, in part, in the Economics & System Model (WP6).</p> <p>4. Same view (WP technique) to multiple aspects Same view to multiple aspects has been considered in the Security and Society (WP4) models and Security Risk Model (WP5) and in the Economics & System Model (WP6).</p>
--	--	--



B. Detailed list of Activities in Support to Toolkit Development

Phase	Date	Activity	Participants
1. Interface testing and adaptation	7/3/2014	Telco with Fraunhofer to check a first approach of the user interface for the Toolkit based on the airport models.	DBL, Fraunhofer ISST
2. Discussion on feedback regarding the main interface components	27/6/2014	Telco with Fraunhofer to check the user interface for the airport security models, including info, input and output and the template for the printed report.	DBL, Fraunhofer ISST
3. User interaction and GUI redesign	September - October 2014	Discussion on DBL redesign of the logical structure of the interface	DBL, Fraunhofer ISST
4. Interface testing and adaptation	September - October 2014	Offline exchanges about optimization/remediation actions to be carried out to improve the usability of the interface	DBL, Fraunhofer ISST
5. Interface testing and adaptation	8/10/2014	Telco to review finalised version of tool with implemented model for WP5 and WP6 models	DBL, Fraunhofer ISST
6. Interfaces refinement	16/10/ 2014	Telco on refining the parameters for the Airport Security models.	DBL, Fraunhofer ISST
7. Tool tuning	October - November 2014	Testing the Security Risk Model (WP5) cases: data were collected in order to define the input parameters for two further Airport cases.	DBL, Fraunhofer ISST

C. Detailed list of Validation Activities □

Type	Date	Activity	Participants
1. Stakeholder buy-in	27-28/2/2014	Dissemination and validation Workshop for Airport Security case study, Anadolu University	Turkish civil aviation professionals, Officers from European Commission, Turkish CAA-DGCA (Directorate of General Civil Aviation), Turkish ANSP-DHMI (General Directorate Of State Airports Authority), Airlines, Sabiha Gokcen (Istanbul) airport, Air Traffic Controller's Association (TATCA), researchers and project experts from AU.
3. Calibration	March/April 2014	Pre-analysis activity - Analysing the tool through the expert judge.	Security instructor certified by IATA, Air traffic controller and aviation expert.
1. Stakeholder buy-in 2. Confidence building	4/11/2014	Demo with Application session at the Summit Conference, Bruxelles	Airport Security experts from industry (HP Security Labs), european commission (DG Move) and international organization (IATA) have been involved in the SECONOMICS Policy Toolkit Validation with Aviation Security Stakeholders.
2. Confidence building 4. What-if scenario	21/11/2014	SECONOMICS Tool Anadolu validation workshop, Anadolu University 1. General SECONOMICS studies and Tool presentation, 2. Focused interaction with Tool and participants.	Anadolu Airport Accountable Manager, expert air traffic controller, airport security expert and instructor and former CNS/ATM Safety Manager.
2. Confidence building 4. What-if scenario	1/12/2014	Tool Validation Workshop, Ancona-Falconara Airport 1. To present the final results to airport security stakeholders, 2. To discuss and validate the tool for airport security decision making	Management and Security Board of three different Central Italy medium size airports, i.e. Ancona-Falconara Airport, Perugia Airport, Rimini Airport.

D. Detailed Tables of Results of Tool Evaluation Activities

Qualitative feedback regarding the main UI components

UI components	Description
Model selection	<ul style="list-style-type: none"> Adjustment of the Model Selector representation in the sidebar Improvement of readability of labels for scenario selection
Computation execution	<ul style="list-style-type: none"> Needed revision of the 'Attack Results'/'Calculate Results' commands Adjustment of the positioning of the 'Budget' item (need to move it close by the defender box). Adjustment of the positioning of the 'Iterations' item (need to move it close by the 'Optimal Portfolio' of countermeasure command. It represents a variable affecting the computation) Addition of a 'Reset' command which makes all the fields empty after a calculation is over.
Visualization of the results	<ul style="list-style-type: none"> Revision the table structure and suggestion of a 'tab' structure where the different cases are shown in dedicated tab (see the img Tool_Interface_proposal). Suggestion to increase the dimension of the results table. Change the 'first case' label (e.g. Mid-level traffic) into 'Optimal portfolio' versus the 'Second best portfolio'. Optimal portfolio visualization: revision of the labels of the sections of different security measures (not readable). Or add a legenda.
Other components (e.g. Impact of consequences of the attack)	<ul style="list-style-type: none"> Revision of the defender bullet list. There are items without bullets that might be removed. Revision of the font size of the different titles

Detailed Feedback on Tool Interface

N.	Issue	Description
1	Interface - Input	Insert 'Annual Cost' instead of costs: it is not monthly. It regards both the treatment and the representation of the data
2	Interface - Input	Modify the Deterrence / Detection: expand the table view and modify the High into H, Moderate into M, Low into L.
3	Interface - Input	Insert a new 'Airport Profile' table with descriptive text of the Defender (with traffic volume, i.e. n. ° passengers/Year).
4	Interface - Command	Modify the 'Optimal Portfolio' in 'not-pressed' (default) and pressed (Feedback already present but needing to be improved).
5	Interface - Command	Insert 'Model Iterations' instead of Iterations
6	Interface - Results	Insert a legenda in the results (in order to specify the measures)
7	Interface - Results	Review the presentation of the results (i.e. the rings). In the below part are not easily readable/ understandable.
8	Interface - Visualization	Revise the presentation of the cost numbers (adopt a standard representation, e.g. 5.000.000, 00)
9	Interface - Visualization	Remove the 'attack results' table from the interface. It is not an interactive parts, rather a presentation table.
10	Report	<ul style="list-style-type: none"> Modify the font dimension Add project and EU logo Modify the name of the doc: it is not a template but, since it is filled in. We



SECONOMICS

		<p>could name it 'Report'</p> <ul style="list-style-type: none"> - Variables need to be in BOLD - Add a description of the airport (which comes from the input provided in the new 'Airport Profile' table). - Specify that the costs are 'annual costs' - Modify 'the cost of 'preparation costs'' into 'the value' of the preparation costs
--	--	---

Task analysis and evaluation

Tasks		Description
1	Change Airport cost parameter	Issue a: when you manually insert the cost of an airport security measure, the predefined values in the drop-down menu disappear.
		Issue b: when a new security measure is inserted, the new label is loaded in the results' table but it doesn't update in the results' text paragraph
		Issue c: the tool doesn't allow defining less or more than 5 security measures. It may occur that fewer or more than 5 measures are required (up to 8 is suitable for WP1 scenarios).
		Issue d: the addition of new measures should be allowed, i.e. beyond the 5 predefined fields.
5	Save new version of the scenario	<p>Issue e: when a newly created version of the scenario is loaded, the results are not saved. The input tables do contain the data but the results' table is empty. The 'Airport Example' that you have created does contain the results as well. Having both the possibilities could be suitable:</p> <ul style="list-style-type: none"> - saving versions including the results - saving versions which not include the results

E. User interaction and interface design

WP1 contributed to user interaction and GUI design to tool development by also providing an overall redesign of the logical structure of the interface

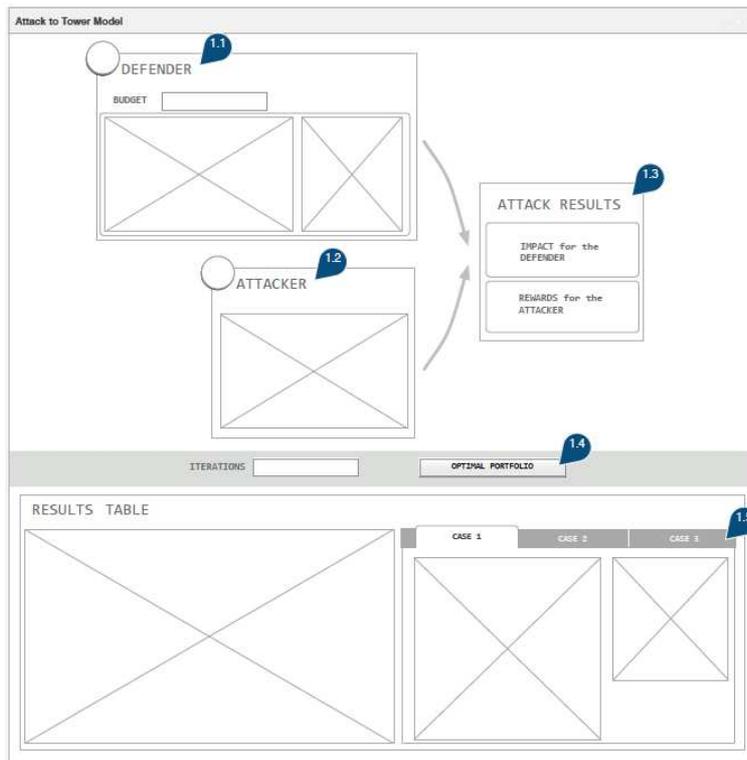


Figure 2: Wireframe proposed for tool GUI redesign

Additional inputs were provided for the GUI redesign:

UI components	Description
a. Input tab - Defender Box	<ul style="list-style-type: none"> - modify the 'Budget' field into 'Security Budget' - add the field 'Average revenue for passenger' (with a predefined parameter which we are investigating at the moment plus the opportunity to insert manual input) - add a further column in the input table where to insert the 'minimum quantity' required beside the 'maximum quantity' - Insert 'Annual Cost' instead of costs: it is not monthly. It regards both the treatment and the representation of the data. - add the field 'Number of passenger /Year' (with the manual input option only)
b. Expert Input sub-tab	- the added value and the scope of including this table it is not clear for us. It seems to us that we require too much complicated contribution to our stakeholders. Moreover we do not exactly understand how it is built, e.g. does number of rows correspond to number of countermeasures?



SECONOMICS

c. Output	- we would select the third option (displayed in the High traffic tab), including the table and the two portfolio.
-----------	--

F. Detailed Tables of Results of Validation Activities

<p>Please indicate below which issues do you consider as strengths or weaknesses about the SECONOMICS modeling approaches and tool for describing the selected domains and explaining the related processes.</p>	
STRENGTHS	WEAKNESSES
<ul style="list-style-type: none"> - The tool allows to focus on emerging security-economics (SECONOMICS) clusters of airports. - Results seem to be quite consistent and solid. - Data collection seems to cover many possible sources. In particular the SECONOMICS media corpus is a highly appreciated. - The variety of security-critical issues and environments that are taken into account in the tool. - The collaborative research approach that covers government, academia and the private sector, gives an holistic view in the areas covered. - The purpose of increasing airport security standards to the highest levels. - It can be useful for reducing predictable behaviours. - The tool provides an easy way to calculate the impact of the different security measures selected. - It has an attractive and simple visual design and provides a useful report including all the information taken into account. - The approach looks fine and effective: costs, deterrence issues and impact are considered. - The tool is basic but it does rely on a valuable set of information as input parameter. - Security is a very complex problem but the tool approach is very simple and cover all the possibilities. 	<ul style="list-style-type: none"> - The attacker profile needs to be enhanced: cyberattacks somehow show a trend of more complex attacks. - Use cases could be considered limited. - Tool deployment to stakeholders real cases is not yet clarified and presented. - The difficulty of evaluating the impact of an attack in a real-world scenario. - Unpredictable behaviours are difficult to include and to use for getting reliable figure and information. - The 'salience' concept is not so immediate and need to be further explained. - Need to consider that equipment can have huge initial costs and than much lower annual costs. This issue affects investement decision. - Human factors are not fully covered in the model as a parameter.
<p>Please indicate below any things you would like to suggest for future exploitation of the SECONOMICS project results and any concerns you have about the suitability of the project modeling approaches to support socio-economic security decision making.</p>	
SUGGESTIONS	CONCERNS



SECONOMICS

- It could be interesting to integrate an automatic data collection and normalization tool.
- As the results are published there would be the need to review the ways they add value for the stakeholders after a few months.
- Security costs need to be shared and contributed by both public and private actors.
- Airport security costs do represent more than the 5% of the annual budget.
- Take into account the daily and weekly traffic peaks rather than the annual flow of passengers.
- It could include several parameters (dynamic, interactive, casual and causal) that also affect the analysed security risks.
- The tool should allow to compare the report of same situation with different combinations of security measure implemented.
- The tool should be capable to cover multiple attack vectors.
- Local indicators can be added for more realistic results,
- In the output section, the graphics, titles, axes, units and labels must be clearly given,
- A detailed user manual may be prepared with samples and tutorials.
- The parameters should be given for the users as a drop-down menu. When the users entered wrong parameters, there should be pop-up tutorials that explains the situation. After running and seeing the wrong input selection makes the time wasting.
- Tool should be available for all kind of computer software infrastructures and provide easy setup procedures.
- Iteration number effect should be identified clearly. It takes more time when selected higher iteration numbers.

- The models can result to be too strictly related to a particular use case and they cannot be generalized in an easy and maybe industrial way.
- The adaptation of the SECONOMICS procedure and practice to different environment could be critical. The models are too much use-case related and the risk is that this could bring to an oversimplification of the attended results in different domains.
- The results seem to not be effectively used.
- The reference National and International security regulations are critical to be considered and integrated into the modeling approach.
- There might not be sufficient security investments to justify the valorization of the SECONOMICS tool.
- The tool should be aware that similar security measures can have different impact depending on the use of private/public security.



SECONOMICS

G. Policy Paper

Martina De Gramatica, Fabio Massacci, Woohyun Shim, Alessandra Tedeschi, Julian Williams (2015)
“IT Interdependence and the Economic Fairness of Cyber-security Regulations for Civil Aviation”.