SECONOMICS

D3.5 - Tool Validation

R. Munné, (ATOS), M. Pellot (TMB)

Pending of approval from the Research Executive Agency - EC

Document Number	D3.5
Document Title	Tool Validation
Version	1.0
Status	Final
Work Package	WP 3
Deliverable Type	Report
Contractual Date of Delivery	31.01.2015
Actual Date of Delivery	31.01.2015
Responsible Unit	ATOS
Contributors	TMB, UNITN, NGRID, DBL
Keyword List	urban transport, security, use case, tool validation
Dissemination level	PU

SEVENTH FRAMEWORK PROGRAMME

Security Economics: Socio economics meets security

SECONOMICS Consortium

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

1	UNIVERSITÀ DEGLI STUDI DI TRENTO	Università Degli Studi di Trento (UNITN) 38100 Trento, Italy www.unitn.it	Project Manager: prof. Fabio MASSACCI Fabio.Massacci@unitn.it
2	DEEPBLUE	DEEP BLUE Srl (DBL) 00193 Roma, Italy www.dblue.it	Contact: Alessandra TEDESCHI Alessandra.tedeschi@dblue.it
3	Fraunhofer ISST	Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., Hansastr. 27c, 80686 Munich, Germany http://www.fraunhofer.de/	Contact: Prof. Jan Jürjens jan.juerjens@isst.fraunhofer.de
4	Universidad Rey Juan Carlos	UNIVERSIDAD REY JUAN CARLOS, Calle TulipanS/N, 28933, Mostoles (Madrid), Spain	Contact: Prof. David Rios Insua david.rios@urjc.es
5	1495 UNIVERSITY OF ABERDEEN	THE UNIVERSITY COURT OF THE UNIVERSITY OF ABERDEEN, a Scottish charity (No. SC013683) 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	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
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	26/11/2014	Draft	R. Munné (ATOS); M. Pellot (TMB)	Final TOC
0.2	04/01/2015	Draft	R. Munné (ATOS); M. Pellot (TMB)	Final draft
0.3	20/01/2015	Draft	E. Chiarani (UNITN) ; A. Pollini (DBL); R. Munne (ATOS) ; M. Pellot (TMB)	Second final draft incorparating inputs form quality check and scientific review. Addition of some KPI's data.
0.4	28/01/2015	Draft	F. Massacci (UNITN); R. Munné (ATOS)	New draft version according requested changes from global review of deliverables
0.5	30/01/2015	Draft	R. Munné (ATOS)	Appendix A reviewed to homogenize presentation with other use cases.
0.6	30/01/2015	Draft	R. Ruprai (NGRID), F. Massacci, W. Shim (UNITN)	Appendix A minor revisions following all case study reviews. Minor changes to document footer. Dissemination Level changed to PU.
1.0	30/01/2015	Final	R. Munné (ATOS)	Final version ready for submission

INDEX

Executive summary

This report presents the toolkit validation process and policy guidelines for the Urban Transport.

The toolkit has been integrated by the Tool Support work-package who has developed the interface and integrated the mathematical models developed by the Security Risk Models technical work-package based on the selected public transport scenarios, pickpockets and fraud.

WP3 has provided support for the development and integration of the models into the tool in the different development phases (interface testing and adaptation, tool tuning and interfaces refinement).

The toolkit has been introduced to the 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. This practice is based on four activity types: 1) Introduction and buy-in by key stakeholders; 2) Familiarization and Confidence building; 3) Calibration; 4) What-if scenario & refinement.

Finally, a validation step on the toolkit has been done, with the participation of stakeholders from the public transport domain (Barcelona regional police in charge of security in public transport, other public transport operators, Barcelona Metro security area and the security commission from the UITP association). They have participated in two workshops for the validation of the SECONOMICS toolkit, and also in a panel during the SECONOMICS Summit activity. All these activities have provided very useful feedback on the toolkit and some interesting policy insights.

The most remarkable results from the validation is that the toolkit provides the capability to estimate how many and the type of resources to face the threats, calculates the appropriate costs of the measures for each scenario considered and provides support about costs and benefits while considering the reaction of smart attackers.

However, the model has also some drawbacks, as it is a static model that does not consider variations during the day, and even types of days (labour, weekend), or variations on the types of measures to apply to a specific scenario. It also requires a consultant support to introduce new models for other scenarios, or the characteristics for other operators. The model is not network enabled, currently it is only exploitable at station level in the toolkit, even the mathematic model is multi station, but it would require a very long time to effectively calculate the required resources for the multi-station model. However this would not be an important drawback as this is process would be done periodically (probably only once a year).

For the policy insights, one of the most important and transversal is the adaptability of the offenders that act in many public transport lines in Europe. They mostly belong to transnational professional criminal organizations, and are characterized to have a high degree of adaptability. This must be considered at the European level for the coordination against threats in public transport, but not only there, as these organisations are not limited to the public transport space.

1. Introduction

1.1 Scope of report

This report describes the evaluation process for the SECONOMICS toolkit with the selected models for the public transport use case, developed during the third year of the project. From the models developed and validated during the second year, that have been implemented into the SECONOMICS toolkit a validation process has been carried out with the same public transport stakeholders that were involved in the previous steps.

1.2 Report Objectives and Results

The objectives and results presented in this report are the following:

- To describe the “Good Practice” for the exploitation of science based policy models and how they can be introduced and used effectivelly;
- To describe the validation activities performed;
- To describe the weak and strong points of the tool;
- To describe the policy insights collected during the validation process;
- To describe the trends and the impact on the toolkit of future and emerging threads.

The validation has been performed by the urban transport stakeholders and they provided very useful feedback about the applicability of the toolkit in the urban transport scenario (user acceptability, domain suitability and system usability). Also some inputs about desirable future developments of the SECONOMICS toolkit have been collected.

2. Support to Toolkit Development

The models developed for the Urban Transport Use Case, described in D3.4 [1] were, implemented in the toolkit with the collaboration of the technical work packages (WP4, WP5 and WP6) and WP8. In the case of Urban Transport, only the Risk Model (WP5) was implemented in the final tool, as the Social Model (WP4) is based in findings from the media analysis (local and national newspapers), and from the security incidents reported at TMB, and therefore, it is not feasible to be automated in the final tool.

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

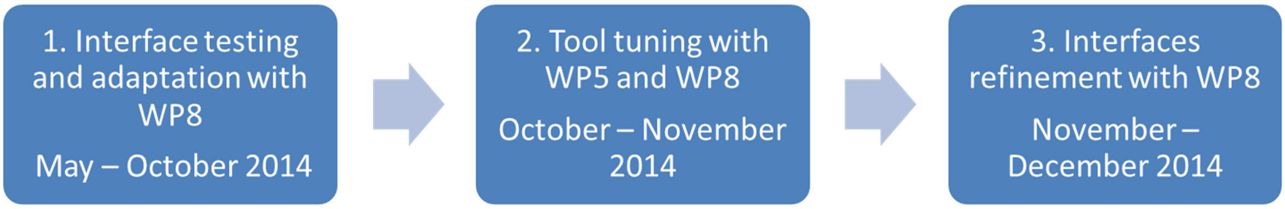

1. Interface testing and adaptation with WP8
May – October 2014
2. Tool tuning with WP5 and WP8
October – November 2014
3. Interfaces refinement with WP8
November – December 2014

Figure 1 Support to Toolkit development process

1. Interface testing and adaptation:
   These activities were done in collaboration with WP8, Tool Support, based on the previous work done in the development of the toolkit interfaces for the Airport models. The activities in this phase took place between May and October 2014. The evaluation of the first proposal for the interface was quite positive as it was based in the infographics developed as part of the models evaluation. These infographics were already known by the stakeholders, as they were presented during the model validation activities.

2. Tool tuning:
   These activities were done after the completion of the interface design, with the first versions of the tool that implemented the models developed in collaboration with WP5, Risk Models, for the Urban Transport Uses Case. This tuning was done in collaboration with WP8, who developed the interface, and WP5. During this phase, specification and explanation of the meaning and suggested values of values for the parameters for the Fare evasion model was required.
   The activities in this phase took place between October and November 2014.

3. Interfaces refinement:
   This phase took place with in parallel with the toolkit validation workshops as part of the direct experience and feedback received during these activities. This involved the suggestion to hide some parameters only suitable for experts that should be visible under an “Experts mode” view. The activities in this phase took place between November and December 2014.

A detailed list of activities can be found under “Appendix B. Detailed list of Activities in Section 2 (Support to Toolkit Development)”.

A detailed view of Tool infographics can be found under “Appendix F. Updated Infographics”.

3. 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 Public Transport use case for the exploitation of the results is composed by two dimensions, the local dimension, represented by the local stakeholders of TMB, including other transport operators in Spain, and the European dimension, represented by the International Association of Public Transport (UITP) as the main organisation grouping stakeholders in the Public Transport arena in Europe and worldwide.

This practice is structured in four main types of activities, as shown in Figure 2 below:

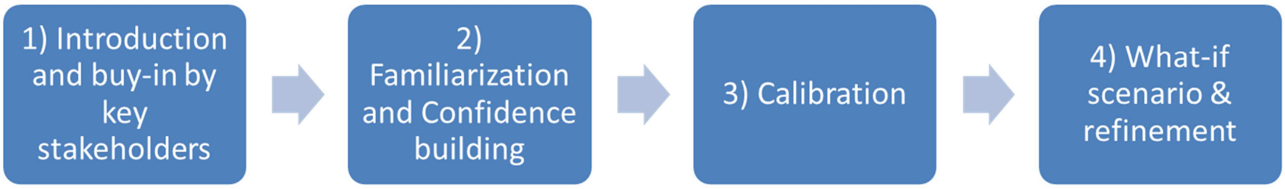

1) Introduction and buy-in by key stakeholders
2) Familiarization and Confidence building
3) Calibration
4) What-if scenario & refinement

Figure 2 Activities for Exploitation of Science-Based Policy Models

1) **Introduction and buy-in by key stakeholders**: This activity has been important during the collection of requirements and during the beginning of the modelling for defining the project goals, getting preliminary feedback and gaining understanding from our stakeholders. It provided the description of the public transport scenarios (Indicators of economic crisis; Fare evasion; Graffiti; Pickpockets), covered in D3.3 [2], and the reasons to select the scenarios to be modelled and deployed into the SECONOMICS Toolkit, covered in D3.4 [1].

2) **Familiarization and Confidence building**: This activity has covered the explanation of the selected public transport models and the description of model characteristics previous to the implementation of the models in the toolkit, explaining what questions the model can or cannot answer, understanding main limitations, what is considered by the model and what is not considered. For the Public Transport use case this included the explanation of the selected models:
   - Societal model:
     - Impact of new (technical) security measures: video surveillance, automatic doors
     - Fraud
   - Security Risk Model:
     - Pickpockets
     - Fraud

3) **Calibration**: This activity has been developed during the modelling phase with the discussions with the technical work packages to elaborate the specific models for the Public Transport at TMB, providing the required information in terms of figures, countermeasures applied in each security scenario, effectiveness of countermeasures and internal organisation of the transport operator. During the toolkit validation activities additional calibration has been performed on the test scenarios, based on the experience of the stakeholders.

4) **What-if scenario & refinement**: This is one of the main activities during the tool validation activities, testing the tool with different input values and checking the different outputs against the experience of the stakeholders.

4. Validation of SECONOMICS Toolkit Exploitation Practice

4.1 Validation activities

The validation activities have been developed along all the project lifetime according the current level of development of the toolkit. At the same time, these validation activities were of different nature according to the scope of audience, and have been developed according the SECONOMICS Practice for Exploitation of Science-Based Policy Models described in section 3 above.

The validation activities in the third Year of the project are based on the validation plan for Local and Regional Transport Case Study, as described in D7.1-Validation Plan [3]. The plan for Year 3 is detailed in Table 1.

Table 1 - Year 3 validation activities

Tool and Guidelines Validation		
M25-M28	M25 – M32	M34
Tool Non-interactive Prototype Evaluation - Consortium Partners (domain and social experts)	Tool and Guidelines Validation trough usage and application to the Scenarios. Consortium Partners (Technical partners, domain experts and End-Users	Tool Live Trials for Guidelines Production and Refinement with transport stakeholders and policy makers - Direct observation, interviews and dedicated Workshops

The specific toolkit validation activities were based on validation workshops with stakeholders. The workshops structure used for the toolkit validation is as follows:

- Introduction
- Security Risk Models approach
- Toolkit Demo + Live Exercise
- Live Exercise with Security Risk Models (What-if)
- Final evaluation

The aim of the sessions was to validate the toolkit for both Security Risk models and for different situations (scenarios of Metro stations).

The Security Risk models that the tool is based on were presented, as well as the tool functionalities. Additionally, some examples were run in the Live Exercise slot, with discussion on the applicability and usefulness of the toll for the specific models and scenarios. The last part of the workshop was dedicated to the collection of feedback on the Security Risk Models approach and on the Toolkit for its Domain applicability and System usability of the Toolkit.

Additionally, as a formal tool for collecting feedback, a quantitative survey was used to check the Toolkit for its Domain applicability and System usability.
A detailed list of the validation activities and the survey used during the validation workshops can be found at "Appendix C. Detailed list of Activities in Section 4.1 (Validation Activities)".

4.2 Validation Results

A total of six expert stakeholders inputs were collected during the validation workshops. The summary of the validation activities can be found below.

Four types of results from the validation activities have been collected: (1) User acceptability of security risks modelling approach, strengths and weaknesses, through a poll; (2) Domain suitability and (3) System usability, collected through surveys in the form of an evaluation questionnaire. Additionally feedback on the (4) Future development of the tools has been also collected in addition to the evaluation questionnaire.

4.2.1 User acceptability for security risks modelling approach, strengths and weaknesses

This feedback was collected using a template to indicate, with free text, the issues considered strengths or weaknesses as well as suggestions and any concerns about the suitability of the modelling approach.

Strengths

- Estimation on how many resources to use:
  - Allows an indicative estimate of how many and what kind of resources to consider in addressing threats.
- Calculation of scenarios costs:
  - Provides a global vision about the effective appropriate costs of the measures and the benefits provided, based on a previous analysis of each scenario.
- Scenario application and adaptation:
  - Facilitates the analysis about behaviours. Once analysed in one point of the transport network it can be extrapolated to other points with similar scenario and behaviours.
  - Proposes a flexible configuration that allows appropriate adaptation to different scenarios and transport operators.
- Decision making support:
  - Given the complexity of the subject and the lack of management, decision making and planning tools in the field of security, any tool provides a support for decision-making in this area.

  - It provides key data and quantifiable variables of interest.
  - Clearly introduces the contrast between costs and benefits and considers the reactions of smart attackers, beyond traditional approaches of immobile and not evolutionary behaviour.
- Miscellaneous:
  - As a concept it is very powerful and crosses many possibilities.
  - Complex mathematics formulas used.

Weaknesses

- Not suitable:
  - From an operational standpoint it is not a practical tool, at least regarding the pickpockets scenario.
  - Requires strong analytical work, which can make you stop using it.
  - To apply the results at the operational level requires consideration of concrete data, not only at spatial level but temporal, since threats do not have a linear behavior over time.
  - Does not give you the option to determine which means are the right ones.
  - The weight of the weaknesses makes it very difficult the real use of the tool in the scenarios studied.
- Hardly adaptable:
  - Hardly scalable to other situations or operators.
  - The adaptation to other scenarios of the same enterprise requires extensive programming.
- Does not take into account other impacts:
  - Does not provide the social impact of the tool, or it should be visible.
  - Other factors should be assessed, not only the economic ones.
  - Falls outside the insecurity perception of the passage, and more specifically of the victims.
- Scope:
  - Only allows you to decide on a point, loses the global view of the operations problems. The model should be applied at network-level not only to a station.
- Complexity:
  - Resources are limited and always shared for several stations or points, so it is difficult to establish the actual costs.
  - Before start filling in the data for the model, some decisions should have been taken before.
  - The complexity of modeling human behavior, and the offender's behavior generates many biases, uncertainty and randomness, which are difficult to correct and include in any tool.

Suggestions

- Start at a higher lever for planning:
  - Probably it would be better to start from a more global view (transport network) to determine which solutions are most appropriate / profitable, and

- then descend to more detailed scenarios (lines -> station).
  - It should have a preliminary step to determine the appropriate resources and cost, and then adapt them to the available budgets at every time.
- Additional things to consider:
  - It must be provided in the analysis any input that enables the end user of the tool: to reduce uncertainty in the result; to facilitate the programming of new scenarios; to be a more dynamic tool.
  - Should consider time slots and type of day (working, festive, etc).
  - The decisions of the attacker (fraudsters, pickpockets) and defender (public transport operator) are taken into account, but the opportunity of crime theory, also known as "Triangle of crime", provides that the causes of any crime depend on: (1) the offender, (2) the security manager and (3) the victim, where the latter may be decisive at the consummation (or not) of the incidence. For this would be useful to include the victim in the tool.
  - It should be allowed the user to add new measures in a simpler way. Even if each measure requires a prior analysis.
  - Input values easier to quantify, because it might be easier from the standpoint of fraud. With the working data it is very difficult to assess the theft and work on the current values.
- Type of output to provide:
  - Give visibility to the social impact generated by the implementation of the tool.
  - To develop the tool potential for prediction, that is, if we have data on number of passengers, cameras, human resources, etc, could infer the probability of attacks.

Concerns

- It is a first step to be enhanced:
  - It is the beginning of a positive tool because it allows consider and justify security measures that are usually implemented with very poor analysis or even no previous analyses.
  - It's a good theoretical model, but there are still many aspects to develop at practical level to be effective.
  - The data and information requested by the tool to include, for example, security measures are the most common, but not the only ones, therefore, it would enhance the effectiveness of the tool (although its complexity) to include more security measures (all) assessing their impact on the "attackers" depending on each case and scenario.
- About the effectiveness of the tool:
  - The application should be able to give a true picture of the problem throughout the year and not once, since in that case it is only valid as a guideline and not as a tool for efficient planning.
  - The first thing businesses to pose is whether it is necessary to invest in security measures, hence the first demand is getting a first look at what happens if nothing is done and then for certain actions (first at network level).

- If threats are taking shape and acquire a large extent, the effectiveness of the measures may not be homogeneous, since the strength and perseverance of the attackers is greater.
- It is based on subjective data and interpretations of behaviour, which creates doubt in its response.

4.2.2 Domain Suitability

This feedback was collected with a questionnaire with pre-set answers of type “Strongly agree”; Rather agree”; “Difficult to say”; “Rather disagree”; Strongly disagree”.

Answers were quite distributed and balanced with an approach to a neutral answer because most of the answers were “rather agree” and “rather disagree”:

- Between neutral and rather agreeing that the SECONOMICS Tool can be used by consultant to model and analyse the case study in support of the policy-makers.
- Rather agree that if consultants create models with SECONOMICS Tool, the models and the results can be understood by policy-makers.
- Rather agree also that the SECONOMICS Tool can be used by policy-makers, at least partially, to model and analyse the case study.
- Rather disagree on the point that the SECONOMICS Tool can be used by policy-makers, in complete independence, to model and analyse the case study.
- Rather disagree on that on that no additional knowledge or research is required to run the SECONOMICS Tool.
- Rather agree that the SECONOMICS Tool can be used in the existing case study processes/ workpractice.
- Rather disagree that the SECONOMICS Tool can be used without major revision of the existing processes/ workpractice.
- Rather agree that the SECONOMICS Tool contributes to a better support for security management in the urban transport public domain.

4.2.3 System Usability

This feedback was collected with a questionnaire with pre-set answers of type “Strongly agree”; Rather agree”; “Difficult to say”; “Rather disagree”; Strongly disagree”.
Answers were quite distributed, but with a greater trend towards rather agreeing on the usability of the tool.

- Most of the answers rather agree that they that I would like to use this tool frequently.
- Between neutral and rather disagree that found the tool unnecessarily complex.
- Most of the answers were between strongly agree and rather agree about that they thought the tool was easy to use.

- Half of the answers strongly disagree and the rest rather agree or rather disagree that they would need the support of a technical person to be able to use this tool.
- Majority of answers between strongly agree and rather agree, that they found the various functions in this tool were well integrated.
- Slightly agree about the thought there was too much inconsistency in this tool.
- Mostly agree that they imagine that most people would learn to use this tool very quickly.
- Respondents found between neutral and rather disagree the tool very cumbersome to use.
- Between neutral and rather agree feel confident using the tool.
- Between neutral and rather disagree found they needed to learn a lot of things before they could get going with this tool.

4.2.4 Future development of the SECONOMICS Tool

This feedback was collected with five specific questions about future developments of the SECONOMICS tool, in the last as part of the questionnaire. Following is a summary of answers collected. The full content of answers can be found at APPENDIX E. Input for future development of the SECONOMICS Tool.

For the stakeholders the most interesting additional features would be (i) the development of additional scenarios functionalities; (ii) the measurement of the impact for some aspects like social or the role of the victim; (iii) other operating functions and analysis, like providing predictive information, network analysis or decision on the optimal resources before deciding the budget and security measures assigned to a given scenario.

Regarding additional data or outcomes to support decision making, the stakeholders suggested (i) additional information on incidents; (ii) information on external factors like dynamics of users, or statistical data based on the operation; (iii) information on the impact of the application of the tool; (iv) information on the most effective time slots to implement the measures, also considering the type of week day.

For additional visualization modalities, the stakeholders requested a report to compare two or more calculations and scenarios, and also to have some economic and operating information from the implementation of the security measures; finally the possibility to filter the results by different variables.

For the question on the interoperability of the SECONOMICS Tool with existing software, the answers were in the scope of integrating external information about incidents and location of existing security measures from some external databases or spreadsheet files.

For additional reports, the request were to provide comparison between models and variants according to the available budget, and also some extended report with additional information with costs, resources and current security situation of the network.

5. Policy Insight from Validation

5.1 Summary of Findings at the Validation

From the validation of societal models (WP4), it was emphasized the need and importance of considering social factors in addressing security challenges both domestic and those of globalisation and growing diversity. Security in urban public transport must consider and address the growing diversity of passengers in particular in communication and training of security personnel. Other important issues also raised during the validation were the need for comprehensive solutions to security issues and the need for security coordination between public transport operators operating various means of transport and also with the security forces, not only at local level but at pan European level too [4].

From the validation of the security risk models and their implementation in the SECONOMICS toolkit, it was highlighted that the security scenario of pickpockets, which is largely in the hands of organized crime, has a high adaptability. Pickpockets are professionals who exploit in their favour:

- It is an opportunity crime
- They work with intelligence
- They work transnationally
- They take advantage of local laws and regulations

In summary, they work with the approach of “cost minimizing with adaptive intelligence”. This is also applicable to other organized threats, e.g. graffiti. It was also mentioned that if threats take shape and acquire a large extent, the effectiveness of the measures may not be homogeneous, since the strength and perseverance of the attackers is greater. The stakeholders rather agreed that the SECONOMICS Tool can be used by policy-makers, at least partially, to model and analyse the case study, but they can’t use it in complete independence, to model and analyse the case study.

5.2 Summary of findings at the Summit Conference

The public transport case had a panel in the SECONOMICS Summit with the contribution of the Head of the Metropolitan Transport Security Area in Barcelona, Mossos d'Esquadra (Catalan Police Dept) and one representative from the UITP Security Commission.

The most remarkable findings at the summit conference were that the attackers adapt their behaviour according the current situation. For example:

- In the case of graffiti, in New York, graffiti painters have changed their behaviour to avoid being identified after painting one train. Once the graffiti is finished, they take pictures of the works, and after that they destroy it to avoid their identification and their relation with that specific act.
- In the case of pickpockets, the law enforcement agencies have detected that they are changing their behaviour according to the changes introduced by the police to fight against them. Pickpockets adapt their behaviour according to the regulations of the specific country they are performing.

Therefore, it is important that the regulations adapt to the attackers changes in an harmonized form across Europe.

Regarding terrorism, it is in the scope of UITP Security Commission (SecCom), but it is not one of their priorities. UITP SecCom is focused on what they call “daily operational security”, which is considered to be the most important issue for the users of Public Transport. Transport operators collaborate with law enforcement agencies to fight against terrorism or any other type of security threat, as the public transport space is part of the public space domain, as the streets are.

5.3 European Coordination

In addition to the Pan-European coordination section on D3.4 [1] from the model validation process, during the validation process the following issues were confirmed.

The scenarios modelled are some of the main important security issues among the European transport operators (important topics addressed by UITP security commission, SecCom), like Graffiti, pickpocketing, fare evasion and anti-social behaviour, that gives passengers a feeling of insecurity.

There is an increase in international “graffiti tourism”. The UITP SecCom informally exchanges information about this topic. There is an EU project kicking-off to design an EU database & formalise exchange for collecting & sharing data (tags, signatures, modus operandi etc.) of international graffiti.

6. New and Emergent Threats

In addition to the Future and emerging threats section in D3.4 [1] from the model validation process, the most important finding during the toolkit validation about new and emergent threats is about the adaptability of existing threats to changes in legislation and regulation. Most of the regulations are local, and the offenders, usually transnationally organized, take advantage of these differences. They go one step ahead of regulators and law enforcement agencies. This is true for pickpockets, graffiti and any other form of organised threats.

Another aspect to take into account is that these organisations are not limited to public transport. Public transport is one of the places where they develop their activities, but not the only one. The same people may act as pickpockets in a metro line during summer holiday season in a touristic city, and later they can move to another city (and country) during the Christmas season to develop their pickpocket activity in the traditional Christmas markets in central Europe.

Regarding the applicability of the risks models, a new threat would require a new mathematical model supporting the characteristics of the attacker and the required countermeasures to be applied and the associated parameters to be considered for the calculations, e.g. hot topics like graffiti and metal theft.

7. Conclusions

The WP3 validation process has allowed the evaluation of the selected models into SECONOMICS toolkit.

The collected feedback through the workshops participation indicates the following:

- The model provides the capability to:

  - Estimate how many and the type of resources to face the threats.
  - Calculate the appropriate costs of the measures for each scenario considered.
  - It provides support about costs and benefits while considering the reaction of smart attackers.
- Some drawbacks of the model are:
  - It is a static model, not considering variations during the day, and even types of days (labour, weekend), or the types of measures to apply to a specific scenario (which requires analytical work to be considered into the corresponding model).
  - It is difficult to be adapted to other scenarios, from the user point of view. It requires a consultant support to introduce new models for other scenarios, or the characteristics for other operators.
  - It does not consider other inputs in the model, like social, or passage and victims perception.
  - It is not network enabled, currently it is only exploitable at station level in the toolkit, even the mathematic model is multi station, but it would require a very long time to effectively calculate the required resources for the multi-station model. However this would not be an important drawback as this is process would be done periodically (probably only once a year).
  - It does not take into account the complexity, like resource sharing among several security scenarios, or the human behaviour.

Briefly, the approach for calculating the best resource allocation for a specific situation is good, but it misses some high level approach to consider the scenario at network level in the toolkit, and the dynamics of a network transport (behaviour changes depending on the time, mobility of attackers along the transport network).
Besides these considerations, the security risk models can be extended to other types of threats where attackers and defenders want to maximise their effectiveness.

Regarding other types of findings one of the most important and transversal is the adaptability of the offenders that act in many public transport lines in Europe. They belong to transnational professional criminal organizations, and are characterized to have a high degree of adaptability. This input must be considered at the European level for the coordination against threats in public transport, and also must be considered as an evolutionary form of the current threats into new forms of threats that are not only limited to the public transport space.

REFERENCES

[1] R. Munné, I. Zaldivar, M. Pelllot, P. R. Guasti, Z. Mansfelodová, J. Cano, A. Tedeschi, A. Pollini, E. Chiarani, F. Massacci, W. Shim and R. Raminder, “D3.4 - Model Validation,” SECONOMICS project, 2014.

[2] R. Munné, M. Pellot, R. Ortega, D. Villegas, M. d. Gramatica, W. Shim, E. Chiarani, J. Williams, P. Guasti and Z. Mansfeldova, “D3.3 - Urban public transport requirements final version,” SECONOMICS project, 2013.

[3] F. Quintavalli, V. Meduri, A. Tedesschi, S. H. Houmb, S. Castellví, M. Pellot and R. Ruprai, “D7.1 – Validation Plan,” SECONOMICS project, 2012.

[4] Z. Mansfelodová, P. Guasti, D. Gawrecká, T. Lacina, M. de Gramatica, W. Shim, A. Tedeschi, A. Pollini, J. Williams, U. Turhan, B. Acikel, R. Munné, M. Pelllot and R. Raminder, “D4.5 - Price of Security. Comparative analysis of public attitudes to security and acceptance of risk,” SECONOMICS project, 2015.

APPENDICES

A. Assessment of Project KPI for the Scenario

ID	Short Name	Key Performance Indicator value
1	*METHODOLOGY and GUIDELINES for POLICY MAKERS* *[Scale 1-5]*	3. **Explicit linkage of produced artefacts:** There is an explicit linkage with the Security and Society models produced from the study of security factors at TMB. 4. **Formal linkage of produced artefacts** There is a formal linkage of the toolkit with the Security Risk models implemented. 5. **"Local" Usability of methodology in producing artefacts:** The Toolkit only requires to have a specific knoledge on the specific security models for urban public transport (pickpockets and fare evasion). The user does not need to know the details about the implementation of the model.
2	MODELLING NOTATIONS and LANGUAGES for SYSTEMS DESCRIPTIONS *[Scale 1-5]*	4. **Formal characterization of constructs:** The mathematical Security Risk models are designed with the specific security measures and behaviours of attackers and defenders. 5. **"Local" Usability of construct:** The construct is transparent to the user. Only needs to understand about the number of iterations to have a more precise set results.
3	ALGORITHMS and COMPUTATION for ECONOMICS and RISK ASSESSMENT *[Scale 1-4]*	3. **Computer Aided Computation.** There is a fully automatic or interactive implementation of the security risk model algorithms implemented in the toolkit. 4. **Formal or operational evidence of efficiency.** A full precise result is only possible after running thousands of iterations, so it is not possible to get accurate results on the fly. Immediate results can be obtained with just a few iterations, but they are not precise enough.
4	*TOOL*	The tool supports the methodology and computation so the same criteria apply to the supported artefacts. It is fully integrated with methodology.
5	USAGE POTENTIAL *[Scale:* *Applied on the case study 1-4* *Requiring Human Effort 1-3]*	**The research technique can be applied on the case study** 2. Results can be understood by the stakeholder for the Security and Society models 3. Can be done by the stakeholder for the Security Risk models 4. Can be done by the stakeholder, in complete independency, but it is not intended to be used for supporting decision making **Required human effort** 2. Equivalent to manual approach for the Security and Society models 3. Saves effort for Security and Society and Security Risk models
6	INNOVATION POTENTIAL *[Scale 1-4]*	3. The technique can be used by revising the existing processes for Security and Society and Security Risk models.

ID	Short Name	Key Performance Indicator value
7	CASE STUDY REPRESENTATIVENESS *[Scale:* *Detail of Investigation 1-4* *Facets considered in the Scenario 1-4]*	**Detail of investigation** 2. Empirical exercise (e.g. with students) to simulate steps. This was acomplished with the Security and society model with the analysis of national media for the related security aspects. 3. Empirical exercise by stakeholders to simulate fractions of the process. This was the level reached with the Security Risk Models, as the model implemented in the tool is able to calculate the optimal resources for one station, but not for the whole tansport network. **Facets considered in the scenario** 2. Several aspects for a considered scenario in the Security and Society model (awarenes and social acceptance of existing and new security measures) 3. Multiple views to a single aspect. Fraud scenario analized form the Security and Society model and from the Security Risk model. 4. Same view to multiple aspects. Security Risk models applied to Fraud and Pickpockets scenarios

B. Detailed list of Activities in Section 2 (Support to Toolkit Development)

Table 2 - Detailed list of activities for Toolkit development support

Phase	Date	Activity	Participants
1. Interface testing and adaptation	23/5/2014	Telco with Fraunhofer to check a first approach of the user interface for the toolkit based on the airport models.	TMB, Fraunhofer ISST
1. Interface testing and adaptation	1/8/2014	Telco with Fraunhofer to check the user interface for the pickpockets model, including info, input and output and the template for the printed report.	ATOS, TMB, Fraunhofer ISST
1. Interface testing and adaptation	September - October 2014	Adaptation of templates for printed reports for Pickpockets and Fare evasion models.	ATOS, TMB, Fraunhofer ISST
1. Interface testing and adaptation	22/10/2014	Telco to review finalised version of tool with implemented model for Pickpockets and Fare evasion.	ATOS, TMB, Fraunhofer ISST
2. Tool tuning	October - November 2014	Off-line exchange of information between participants to tune the Urban Transport models.	ATOS, TMB, Fraunhofer ISST, URJC
3. Interfaces refinement	November - December 2014	Off-line exchange of information between participants to hide some “Expert” parameters for the Urban Transport models.	ATOS, TMB, Fraunhofer ISST, URJC

C. Detailed list of Activities in Section 4.1 (Validation Activities)

Table 3 - Detailed list of Validation Activities

Type	Date	Activity	Participants

1. Stakeholder buy-in	7/6/2012	Requirements and scenarios definition Workshop, Barcelona.
		Urban Public Transport Case Study.
			TMB security area representatives;
			Transport division of Regional police (Mossos d'Escuadra) representatives;
			SECONOMICS Consortium representatives

1. Stakeholder buy-in	7/11/2012	UITP Commission on Security, 14th meeting, Munich. High-level requirements review.	UITP Commission on Security representatives; Representatives form the security area from several european underground urban transport
1. Stakeholder buy-in 2. Confidence building	19/11/2013	"Rail BCN" international fair on railway industry hosted in Barcelona between 19th and 21st November 2013, during professional conferences named "Rail BCN INNOVA". Presentation on the project goals, the transport use case, and the scenarios analysed.	Transport industry representatitives
2. Confidence building	22/11/2013	UITP Commission on Security, 16th meeting, Hamburg. Update of SECONOMICS project progress on the Urban transport case High-level presentation of models development so far	UITP Commission on Security representatives; Representatives form the security area from several european underground urban transport

2. Confidence building
3. Calibration
	19/12/2013	Model validation Workshop, Barcelona.
		Urban Public Transport Case Study.
			TMB security area representatives;
			Transport division of Regional police (Mossos d'Escuadra) representatives;
			Other spanish transport opperators;
			SECONOMICS Consortium representatives

2. Confidence building 3. Calibration	17/2/2014	UITP Commission on Security, 17th meeting, Karlsruhe, at the IT-TRANS International Conference and Exhibition. A summary of the workshop topics was presented, and the feedback was collected	UITP Commission on Security representatives; Representatives form the security area from

Type	Date	Activity	Participants
			several european underground urban transport
3. Calibration	4/11/2014	Toolkit validation Workshop, Brussels. Urban Public Transport Case Study.	Transport division of Regional police (Mossos d'Escuadra) representatives; SECONOMICS Consortium representatives

2. Confidence building	5/11/2014	Seconimics summit, Brussels
		Urban Public Transport Case Study.
			Transport division of Regional police (Mossos d'Escuadra) representatives;
			UITP Commission on Security representatives;
			SECONOMICS Consortium representatives

3. Calibration 4. What-if scenario	9/12/2014	Toolkit validation Workshop, Barcelona. Urban Public Transport Case Study.	TMB security area representatives; Other spanish transport opperators; SECONOMICS Consortium representatives

D. Detailed Tables of Results of Validation Activities According D7.1 – Section 4.2 (Validation results)

The following validation criteria, shown in Table 4 to Table 6 have been applied for the validation of the models, as a development of the initial validation criteria for public transport described in D7.1 [3]:

Table 4 - Urban Transport Validation criteria: User Acceptability

WP3 – Urban Public Transport Case Study: User Acceptability		
SECONOMICS Outcomes	**Validation Criteria**	**Validation Results**
Public transport scenarios Description	- Discussions and brainstorming with national and European stakeholders. - Level of acceptance by stakeholders	The scenarios described in the Urban Public Transport case study were shared and discussed with national (TMB and other national operators) and European stakeholders that participate in the UTIP Security Commission. Stakeholder acceptance was high. The scenarios described can, to an extent, be considered similar between transport operators. This is especially true when considering graffiti and pickpockets. Fraud is also commonplace but varying payment, validation and control systems between operators may lead to different criminal approaches. The scenario titled “the indicators of economic crisis” is relevant to a degree but isn’t necessarily applicable to all transport operators.
Security risk and socio-economic model	- Models are well defined -Effective computation - Models are easy to interpret by the stakeholders and accepted. - Formal evidence of efficiency and effectiveness of models	- The **societal model**. Respondents mostly agreed that the model enabled them to: understand the societal and individual determinations of risk, the perception of danger as well as the acceptance of different forms of asocial behaviour and potential security threats that change temporally. The acceptable level of efficacy the model supported was also agreed upon. There are various opinions on how security measures interact with the passengers’ feeling of safety. The model reduces ambiguity and provides better clarity regarding the current situation. The model was found to be both flexible and suitable for application within this domain. - The **risk model.** Respondents agreed that the model has the potential to

		improve the process of decision making, be utilized in the public transport domain, provide relevant & useful output for tasks and positively influence the task when applied. Respondents also agreed that there are various scenarios that would find the model of use and be called for its use in facilitating them. Respondents agreed that the technical and scientific aspects of the model were sound due to the reduced ambiguity and added usability. This in turn aids the user's understanding of the current situation, enhances their knowledge of the area while also remaining versatile and suitable for application within this domain. The most important criterion identified by respondents was model scalability. The least important was identified as being the level of complexity.
Evaluation tools for transport operators and Guidelines for Policy Makers	- Dissemination of the evaluation tools and guidelines to the relevant stakeholders. - Evaluation and acceptance by stakeholders. - Multi-view perspective	The tools were disseminated to the same stakeholders across the entirety of the project lifecycle to maintain the consistency of the evaluation results. The stakeholders maintained their level of interest and acceptance when participating in the evaluation process across the project life cycle. The multi-dimensional elements of the models and tools, supporting the various perspectives, were very well received by the stakeholders.

Table 5 - Urban Transport Validation criteria: Domain Suitability

WP3 – Urban Public Transport Case Study: Domain Suitability		
SECONOMICS Outcomes	**Validation Criteria**	**Validation Results**
Public transport scenarios Description	- Verification TMB scenarios - Users perception considered. - Stakeholders perspectives represented	The models were verified against the TMB scenarios during the model validation workshops. The answers were relatively positive about the applicability of the model to the urban transport context. It's ability to cover both functional and security requirements were also well received by stakeholders.

Security risk and socio-economic model	-Models are developed based on defined scenarios - Acceptable level of integration of the security, economic and social dimension of scenarios	The majority of the stakeholders agreed in the model having the appropriate scope for the urban transport domain.
Evaluation tools for transport operators and Guidelines for Policy Makers	- Compliance with actual policies, procedures and work practice in the public Transport domain -Phraseology and terminology consistent with the one used in the domain -Non-expert users can apply effectively the tools and the methodology for their scopes	The evaluations tools are compliant with the actual policies, procedures in work practice in the public transport. However the models implemented in the tool were limited to one single station and even then do not take into account dynamic factors (such as mobility within the network). That said, the terminology is correct and understandable by users. - The tool is easy to use and can be used by policy-makers to model and analyse the case study.

Table 6 - Urban Transport Validation criteria: Technical Usability

WP3 – Urban Public Transport Case Study: Technical Usability		
SECONOMICS Outcome	**Validation Criteria**	**Validation Results**
Public transport scenarios Description	- Scenarios give information about TMB threats. - economic and social impact information	The scenarios were developed based on the TMB threats and security parameters The tool provides the economic impact. The social impact is only considered as a model when evaluating salience in respect to new security measures.
Security risk and socio-economic model	- Monitor and control of the key indicators. - The results of models are clearly interpretable. - All the relevant information is presented in a clear and usable manner.	It can be useful to reduce predictable behaviours. It is easy to calculate the impact of selected counter measures. The tool provides a report that includes all the information that is used for the calculations.
Evaluation tools for transport operators and Guidelines for Policy Makers	- Well defined, non-redundant and clear methodology steps - Learnability of methodology in producing and linking various artefacts	- The tool is not complex to use. - There is no need for the support of a technical expert to be able to use the tool. The functions found in the tool are well integrated. No extensive learning is necessary before using the tool.

E. Input for future development of the SECONOMICS Tool

Full content of the answers provided for the questions about future development of the SECONOMICS tool. This detail of answers corresponds to the summary of answers presented in section 4.2.4 Future development of the SECONOMICS Tool.

Q1. Would you be interested in additional functionalities? If so, please specify which ones

- Development of scenarios functionalities:
  - It should be able to connect or interact between different scenarios simultaneously.
  - To build easily other scenarios or casuistry.
- Impact measurement:
  - To assess the social impacts.
  - Measure the consequences, in number and quality, of the incidents that are avoided.
  - Include the role of the victim in the prevention / deterrence of fraudster / pickpocket.
- Other operating functions and analysis:
  - To provide predictive information on possible attacks based on available data from stations.
  - Additional operating functions, besides the information on security resources to be allocated.
  - Network analysis. Conclusions for guidance on the need / desirability of implementing certain security measures or to continue implanting them if they are already there.
  - To decide the optimal resources and indicative costs before deciding on the budget and security measures.
  - To design other measures than the ones pre-set in the tool.

Q2. Would you need further data / outcomes to support decision making? If so, please specify which ones.

- Incidents data:
  - Number of incidents.
  - Census of incidents.
  - Consequences of incidents.
- External factors:
  - To calculate how the dynamic of the customers (not only the numbers) affects the measures and the final result.
  - I think that would call for statistical data based on the operation, and as a consequence of these results to be able to apply into the SECONOMICS tool.
- Tool impact
  - Missing data of social impact generated by the implementation of the tool.
  - Clear comparative data between the situation of doing nothing and the various measures to be implemented.
- Time slots /type of day impacts
  - Most effective time slots to implement measures and minimize costs.

  - Consider the type of day (working, weekend).

Q3. 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.

- To create a final report that could compare two or more different calculations and scenarios, besides the totals.
- Yes, I think it should have some economic and operating results of the network.
- To filter by different economic and variables.
- I think the display modes are complete and accurate.

Q4. Would you be interested in tool interoperability with existing software? If so, which software and for pursuing which purposes?

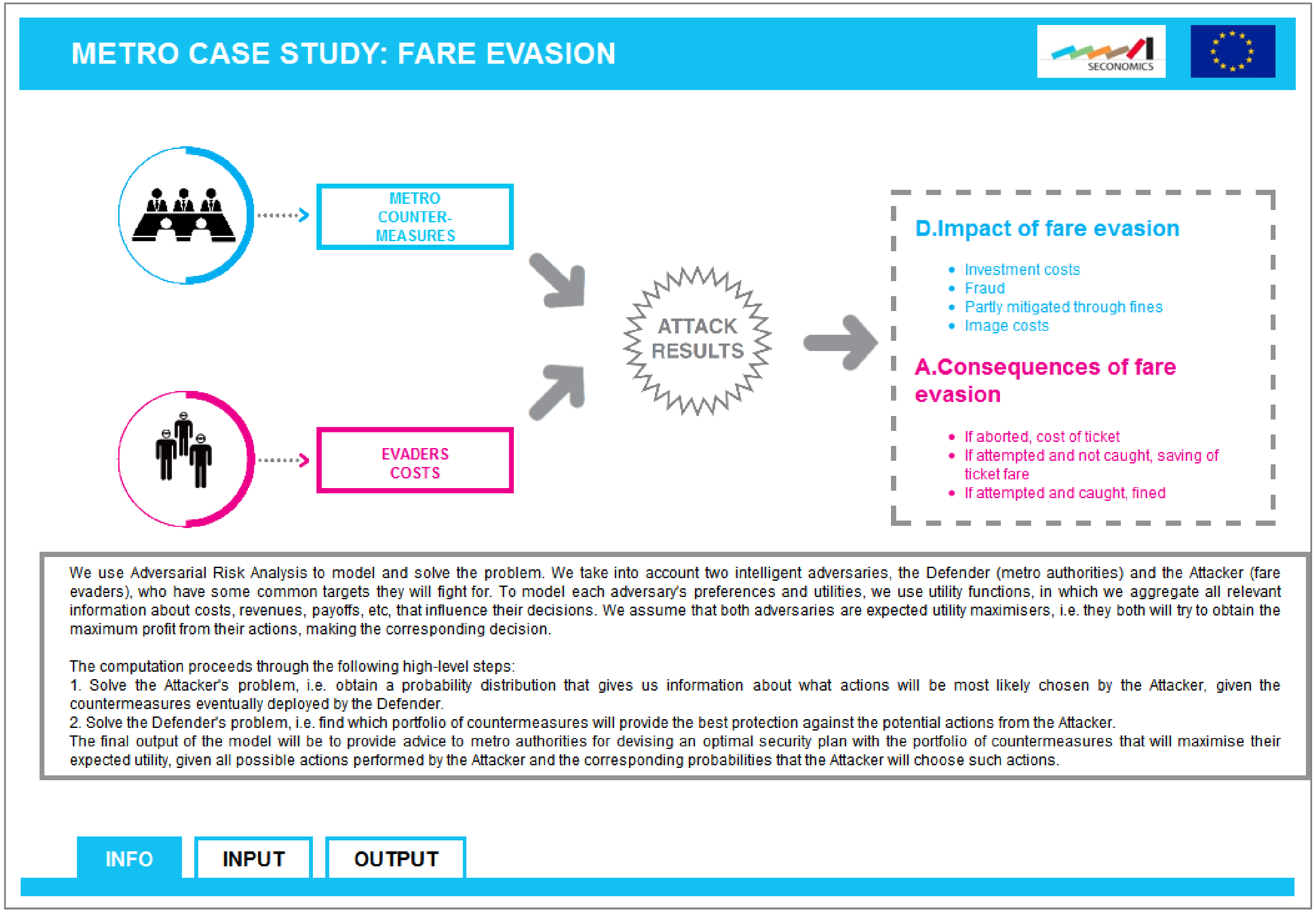
- Simply information collected in, for instance, a spreadsheet document could be integrated into the math calculus.
- It would be interesting that the tool could be feed with the actual and evolving data about the number of incidents, place, date, time, etc. As the number and location of existing security measures.
- Not at the moment, but in case of operating with a software of automated and predictive treatment, it would be interesting.

Q5. Would you be interested in the possibility to automatically get results' report? If so, which kind of outcome would you prefer?

- I think the report is visually pleasant and simply, but provides all the requested information. It can be shown to someone without knowledge about the tool or the calculations made.
- In an application like this, you should get complete results where you could take a radiography of needs according to actual situation of costs, resources and current security situation in the network.
- Comparisons between models and variants of available budget.
- Yes, because it gives consistency to the results presentation.

F. Updated Infographics

Toolkit infographics for Fare evasion model



D.Impact of fare evasion

- Investment costs
- Fraud
- Partly mitigated through fines
- Image costs

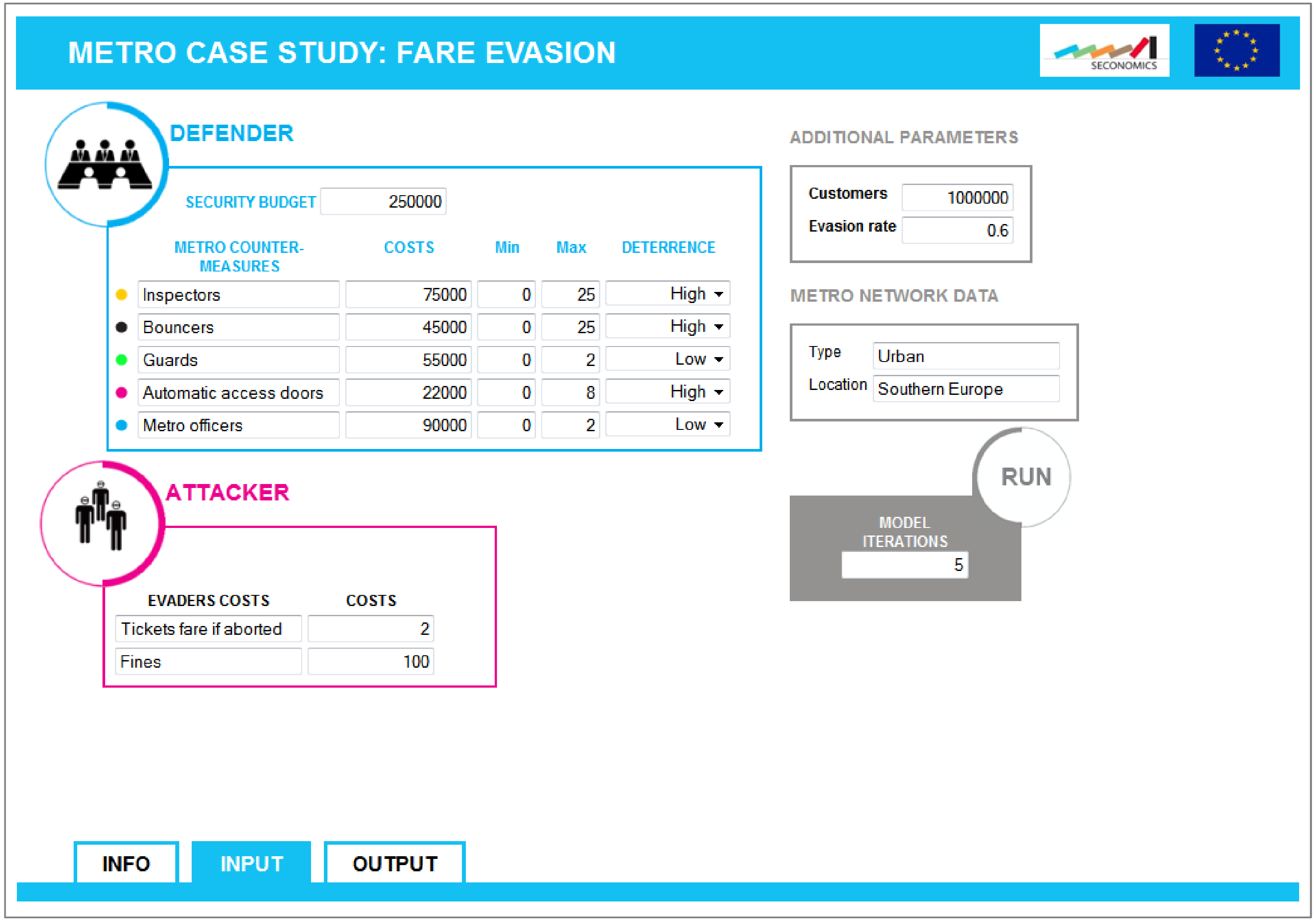
A.Consequences of fare evasion

- If aborted, cost of ticket
- If attempted and not caught, saving of ticket fare
- If attempted and caught, fined

We use Adversarial Risk Analysis to model and solve the problem. We take into account two intelligent adversaries, the Defender (metro authorities) and the Attacker (fare evaders), who have some common targets they will fight for. To model each adversary's preferences and utilities, we use utility functions, in which we aggregate all relevant information about costs, revenues, payoffs, etc, that influence their decisions. We assume that both adversaries are expected utility maximisers, i.e. they both will try to obtain the maximum profit from their actions, making the corresponding decision.

The computation proceeds through the following high-level steps:
1. Solve the Attacker's problem, i.e. obtain a probability distribution that gives us information about what actions will be most likely chosen by the Attacker, given the countermeasures eventually deployed by the Defender.
2. Solve the Defender's problem, i.e. find which portfolio of countermeasures will provide the best protection against the potential actions from the Attacker.
The final output of the model will be to provide advice to metro authorities for devising an optimal security plan with the portfolio of countermeasures that will maximise their expected utility, given all possible actions performed by the Attacker and the corresponding probabilities that the Attacker will choose such actions.

Figure 3 Information Tab for Fare evasion model



METRO CASE STUDY: FARE EVASION

DEFENDER

SECURITY BUDGET 250000

	METRO COUNTER-MEASURES	COSTS	Min	Max	DETERRENCE
●	Inspectors	75000	0	25	High
●	Bouncers	45000	0	25	High
●	Guards	55000	0	2	Low
●	Automatic access doors	22000	0	8	High
●	Metro officers	90000	0	2	Low

ATTACKER

EVADERS COSTS	COSTS
Tickets fare if aborted	2
Fines	100

ADDITIONAL PARAMETERS

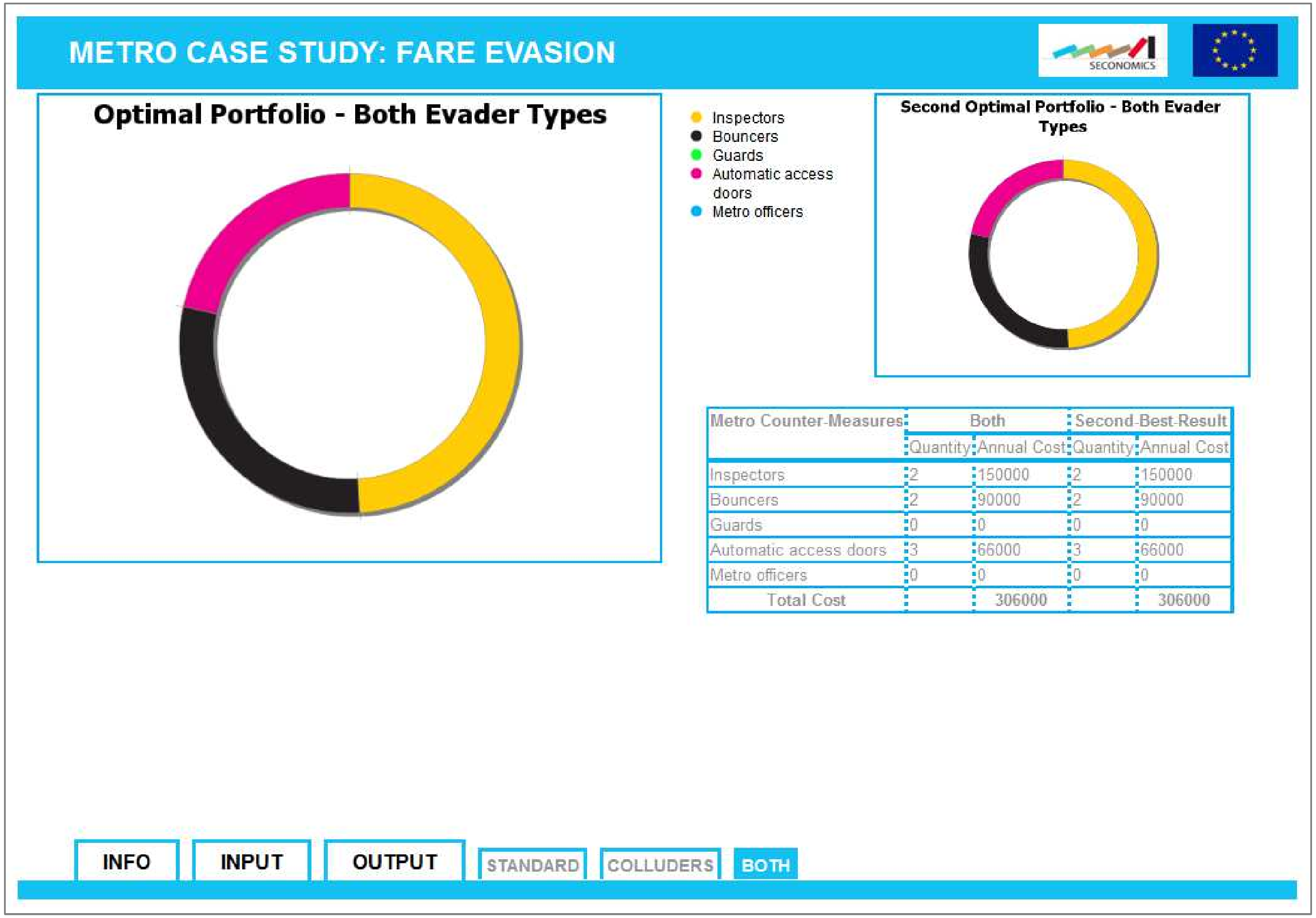
Customers	1000000
Evasion rate	0.6

METRO NETWORK DATA

Type	Urban
Location	Southern Europe

MODEL ITERATIONS 5

Figure 4 Input Tab for Fare evasion model



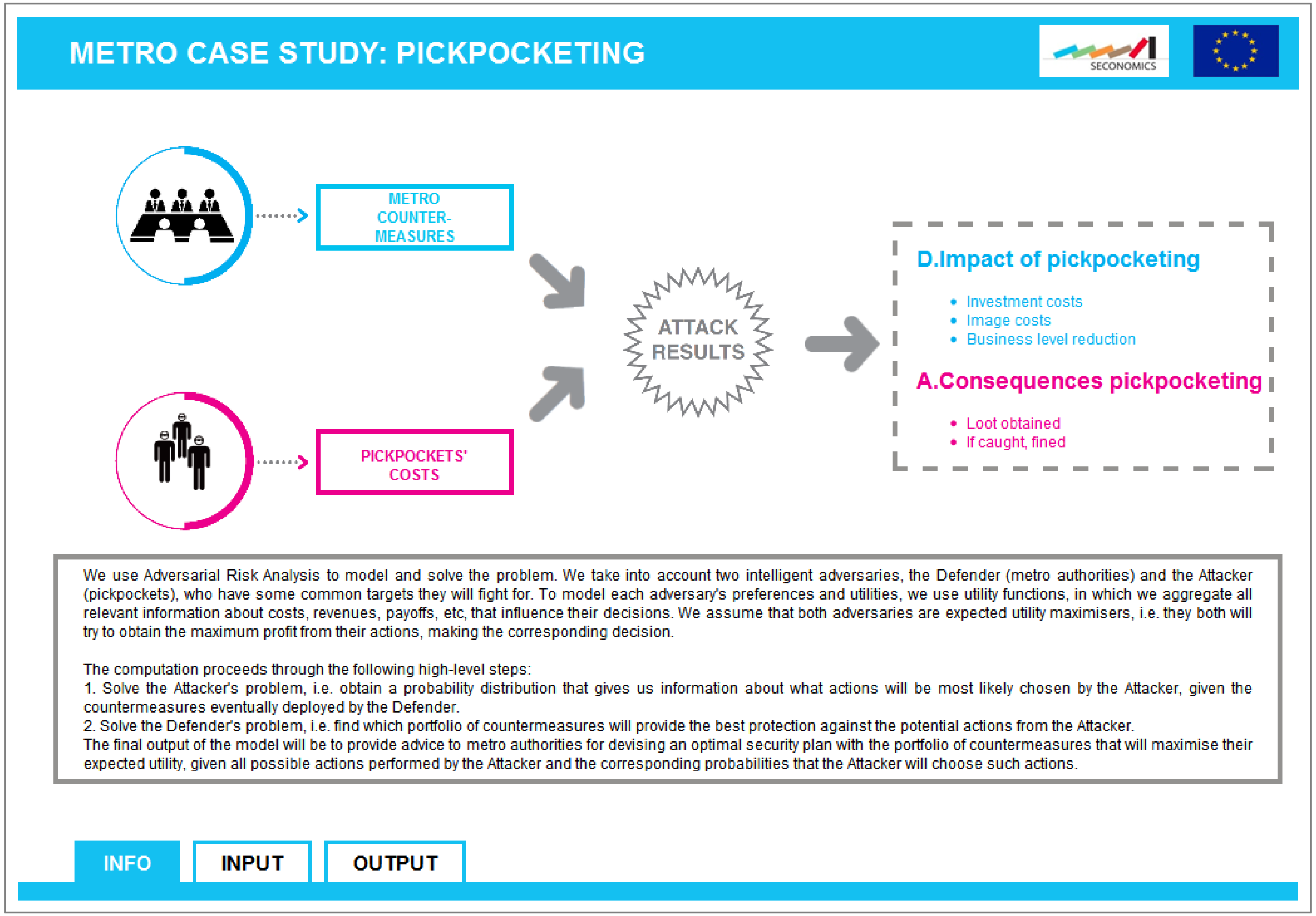
METRO CASE STUDY: FARE EVASION

Optimal Portfolio - Both Evader Types
● Inspectors
● Bouncers
● Guards
● Automatic access doors
● Metro officers
Second Optimal Portfolio - Both Evader Types

Metro Counter-Measures	Both		Second-Best-Result	
	Quantity	Annual Cost	Quantity	Annual Cost
Inspectors	2	150000	2	150000
Bouncers	2	90000	2	90000
Guards	0	0	0	0
Automatic access doors	3	66000	3	66000
Metro officers	0	0	0	0
Total Cost		306000		306000

Figure 5 Output Tab for Fare evasion model

Toolkit infographics for Pickpockets model



METRO CASE STUDY: PICKPOCKETING

D.Impact of pickpocketing

- Investment costs
- Image costs
- Business level reduction

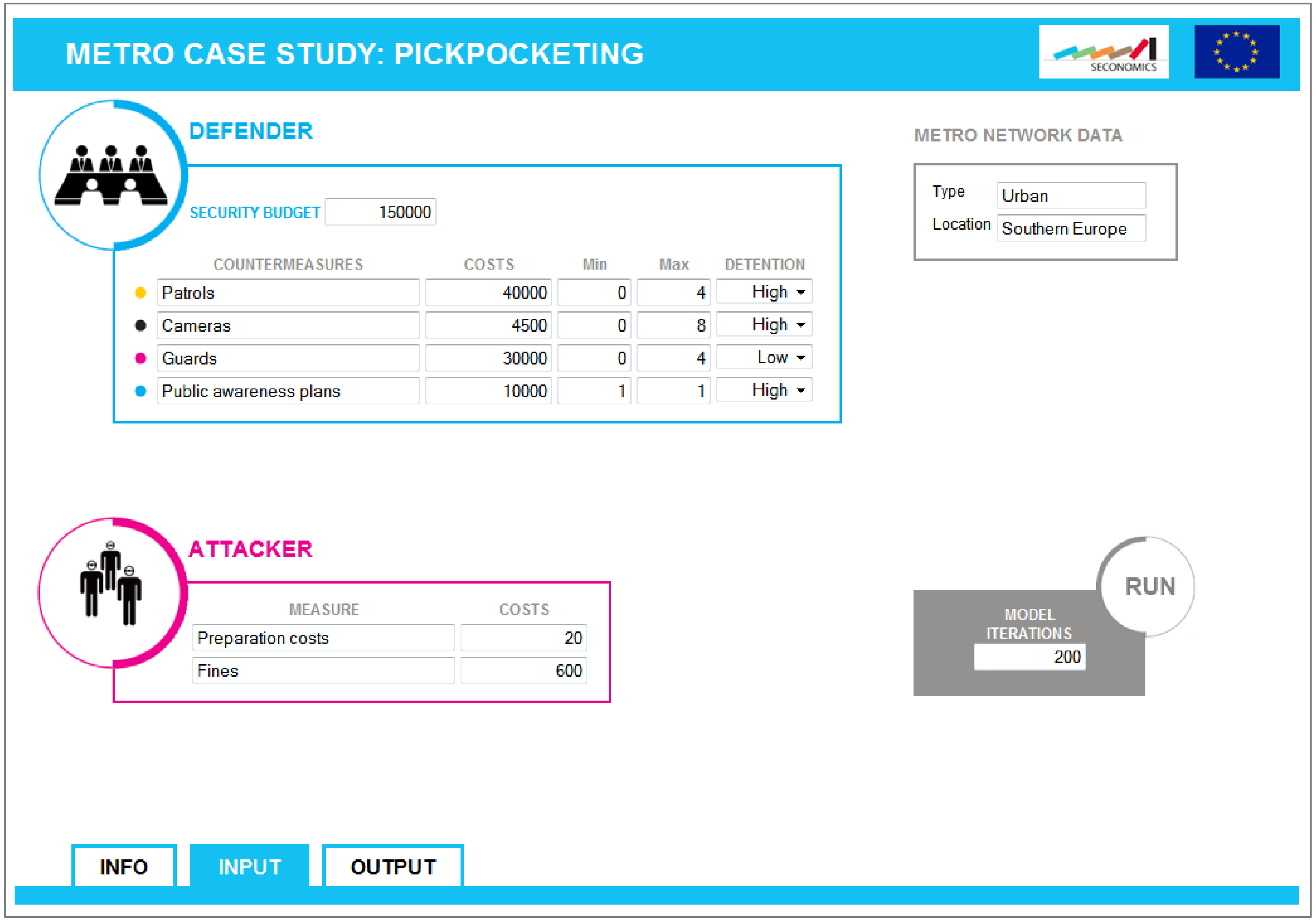
A.Consequences pickpocketing

- Loot obtained
- If caught, fined

We use Adversarial Risk Analysis to model and solve the problem. We take into account two intelligent adversaries, the Defender (metro authorities) and the Attacker (pickpockets), who have some common targets they will fight for. To model each adversary's preferences and utilities, we use utility functions, in which we aggregate all relevant information about costs, revenues, payoffs, etc, that influence their decisions. We assume that both adversaries are expected utility maximisers, i.e. they both will try to obtain the maximum profit from their actions, making the corresponding decision.

The computation proceeds through the following high-level steps:
1. Solve the Attacker's problem, i.e. obtain a probability distribution that gives us information about what actions will be most likely chosen by the Attacker, given the countermeasures eventually deployed by the Defender.
2. Solve the Defender's problem, i.e. find which portfolio of countermeasures will provide the best protection against the potential actions from the Attacker.
The final output of the model will be to provide advice to metro authorities for devising an optimal security plan with the portfolio of countermeasures that will maximise their expected utility, given all possible actions performed by the Attacker and the corresponding probabilities that the Attacker will choose such actions.

Figure 6 Information Tab for Pickpockets model



METRO CASE STUDY: PICKPOCKETING

DEFENDER

SECURITY BUDGET 150000

	COUNTERMEASURES	COSTS	Min	Max	DETENTION
●	Patrols	40000	0	4	High
●	Cameras	4500	0	8	High
●	Guards	30000	0	4	Low
●	Public awareness plans	10000	1	1	High

METRO NETWORK DATA

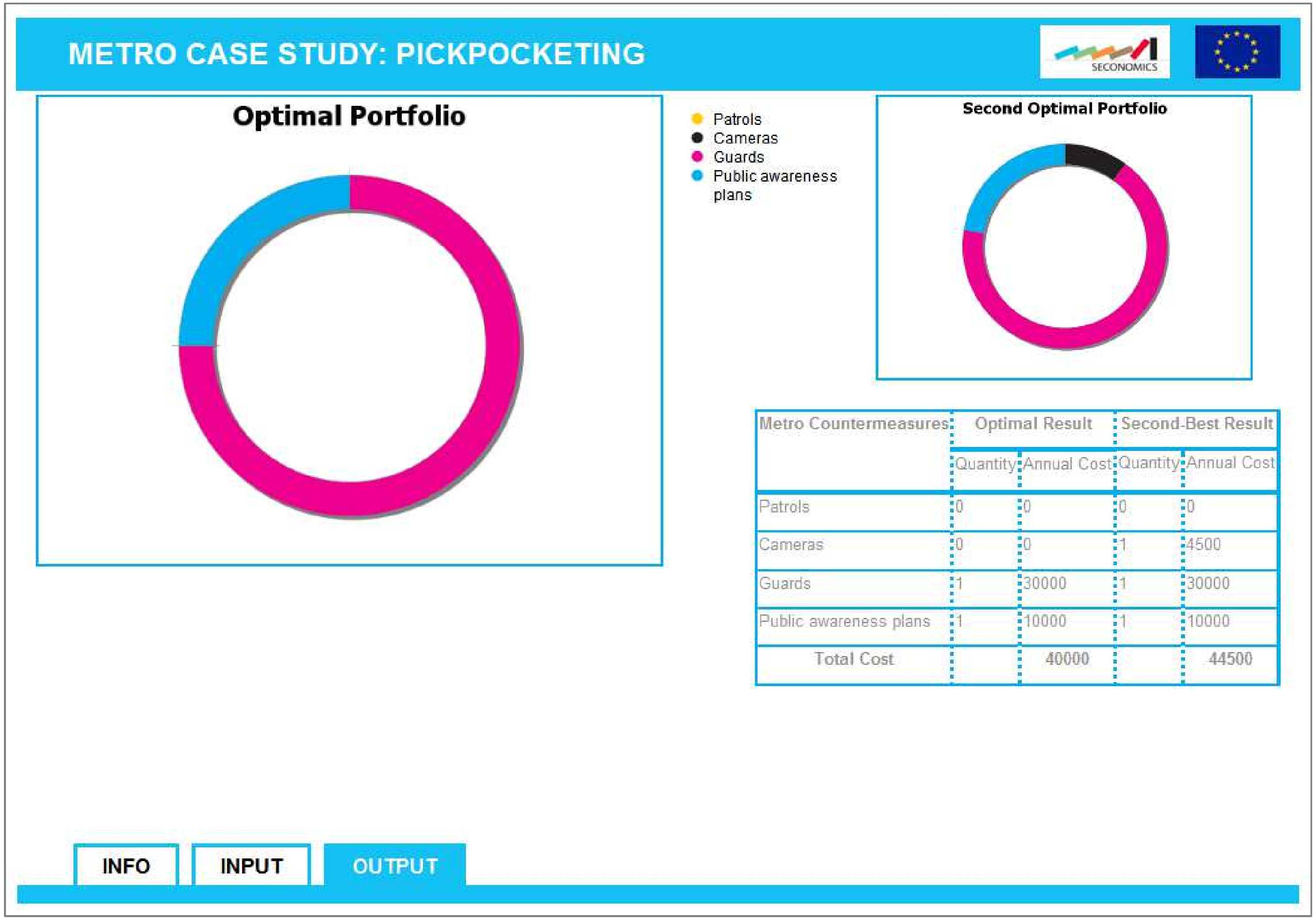
Type	Urban
Location	Southern Europe

ATTACKER

MEASURE	COSTS
Preparation costs	20
Fines	600

MODEL ITERATIONS 200

Figure 7 Input Tab for Pickpockets model



Metro Countermeasures	Optimal Result		Second-Best Result	
	Quantity	Annual Cost	Quantity	Annual Cost
Patrols	0	0	0	0
Cameras	0	0	1	4500
Guards	1	30000	1	30000
Public awareness plans	1	10000	1	10000
Total Cost		40000		44500

Figure 8 Output Tab for Pickpockets model