SECONOMICS

# D9.10 - Final Exploitation Plan

Jorge López (Atos), Alessandra Tedeschi (DBL), Julian Williams (UDUR), Fabio Massacci (UNITN), Raminder Ruprai (NGRID), Andreas Schmitz (Fraunhofer), Emilio López (URJC), Michael Pellot (TMB), Zdenka Mansfeldová (ISASCR), Jan Jürjens (Fraunhofer)

Pending of approval from the Research Executive Agency - EC

| | |
|---|---|
| **Document Number** | D9.10 |
| **Document Title** | Final exploitation plan |
| **Version** | 1.0 |
| **Status** | Final |
| **Work Package** | WP 9 |
| **Deliverable Type** | Report |
| **Contractual Date of Delivery** | 31.01.2014 |
| **Actual Date of Delivery** | 31.01.2014 |
| **Responsible Unit** | ATOS |
| **Contributors** | ISASCR, UNIDUR, UNITN, NGRID, DBL, URJC, Fraunhofer, TMB |
| **Keyword List** | Exploitation, Framework, Preliminary, Requirements, Policy papers, Models, Methodologies, Templates, Tools, Individual plans, IPR |
| **Dissemination level** | PU |

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)<br>38100 Trento, Italy<br>www.unitn.it | Project Manager: prof. Fabio Massacci<br>Fabio.Massacci@unitn.it |
| 2 | DEEPBLUE | DEEP BLUE Srl (DBL)<br>00193 Roma, Italy<br>www.dblue.it | Contact: Alessandra Tedeschi<br>Alessandra.tedeschi@dblue.it |
| 3 | Fraunhofer ISST | Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., Hansastr. 27c, 80686 Munich, Germany<br>http://www.fraunhofer.de/ | Contact: Prof. Jan Jürjens<br>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<br>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<br>http://www.abdn.ac.uk/ | Contact: Prof. Matthew Collinson<br>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<br>http://www.tmb.cat/ca/home | Contact: Michael Pellot<br>mpellot@tmb.cat |
| 7 | Atos | ATOS SPAIN SOCIEDAD ANONIMA ESPANOLA, Calle Albarracin, 25, 28037, Madrid, Spain<br>http://es.atos.net/es-es/ | Contact: Alicia García Medina<br>alicia.garcia@atos.net |
| 8 | SECURENOK | SECURE-NOK AS, Professor Olav Hanssensvei, 7A, 4021, Stavanger , Norway<br>Postadress: P.O. Box 8034, 4068, Stavanger, Norway<br>http://www.securenok.com/ | Contact: Siv Houmb<br>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<br>http://www.soc.cas.cz/ | Contact: Dr Zdenka Mansfeldová<br>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. Raminder Ruprai<br>Raminder.Ruprai@uk.ngrid.com |
| 11 | ANADOLU ÜNİVERSİTESİ | ANADOLU UNIVERSITY, SCHOOL OF CIVIL AVIATION Iki Eylul Kampusu, 26470, Eskisehir, Turkey | Contact: Nalan Ergun<br>nergun@anadolu.edu.tr |
| 12 | Durham University | The Palatine Centre, Stockton Road, Durham, DH1 3LE, UK | Contact: Prof. Julian Williams<br>julian.williams@durham.ac.uk |

## Document change record

| Version | Date | Status | Author (Unit) | Description |
|---|---|---|---|---|
| 0.1 | 17/12/2014 | Draft | Jorge López (Atos) | Draft shared for review of the consortium |
| 0.2 | 13/01/2015 | Draft | Jorge López (Atos) | All sections have been updated with inputs from partners. |
| 0.3 | 23/01/2015 | Draft | Jorge López (Atos) | Updates of executive summary, approach, market analysis and conclusions. |
| 0.4 | 27/01/2015 | Draft | Jorge López (Atos) | Minor updates and correction of typos. |
| 0.5 | 30/01/2015 | Draft | Elisa Chiarani (UNITN) | Quality check completed |
| 0.6 | 30/01/2015 | Draft | Fabio Massacci(UNITN),<br>Raminder Ruprai (NGRID) | Executive Summary & Introduction sections updated. Other minor changes throughout document |
| 0.7 | 31/01/2015 | Draft | Jan Jürjens (Fraunhofer),<br>Petra R. Guasti (ISASCR) | Clarification regarding tool licensing; Minor changes throughout document |
| 0.8 | 31/01/2015 | Draft | Jorge López (Atos) | Names of contributors added:in the front page. |
| 1.0 | 31/01/2015 | Final | Jorge López (Atos) | Final version with comments addressed. |

## INDEX

# Executive summary

The SECONOMICS exploitation plan provides a summary of the individual and cross project impact of the scientific research undertaken in the project. The SECONOMICS project is founded in an evidence-led approach to security policy. This is often taken to mean a ‘data driven’ approach. However, one of the key results from the modelling work of the project is that without properly formed structural models, the inconsistent information that is sparsely available in the security domain may not provide useful information for proper evidence led policy. The SECONOMICS framework seeks to address this issue by providing a modality of research for the policy maker to build an evidence base. In turn this will allow them to instigate and assess regulatory interventions (presumed to be via national or pan-European public policy) in relation to the security of various aspects of critical infrastructure within the scope of the project.

In addition to the direct impact of the applied industry led research, the project also has a foundational impact on the basic scientific research in the areas of public policy, media content analysis and operations research. This document additionally summarizes these key exploitable results under five main categories:

- Best practices and methods
- Models
- Software components: SECONOMICS Toolkit (including MATLAB implementations of the models)
- Information and analysis produced during the project
- Media Corpus

The following four types of stakeholder groups for further exploitation of these results were identified: policy makers, infrastructure operators, consultancy companies and academic & wider R&D community. Exploitation analysis based on global trends such as increased vulnerability, political concern and growing infrastructure investments indicates good prospects for exploitable results to contribute to various security solutions. Security solutions include segments such as video surveillance, biometrics, access control technologies, CBRN (chemical, biological, radiological, nuclear) detection and perimeter intrusion detection.

The SECONOMICS service portfolio includes several types of results for immediate exploitation: advice on optimal security measures within operators, development of security models for policy makers and deployment services. Most of the results will be exploited immediately by the academic community in courses and new research projects. A significant number of models and results are already adequately developed and are ready for commercialisation and/or to inform national and pan-European policy on security. Examples of these include coding techniques for salience analysis in the media, models for public policy with mandatory and risk-based security investments, and model of public acceptance of security measures.

The consortium has decided to make the SECONOMICS Toolkit available with an open source license in order to boost adoption of the SECONOMICS Good Practice by policy makers. This is in line with the European Commission document titled "Guide to Intellectual Property Rules for FP7 projects" (p. 12).

# 1. Introduction

This report represents the final overall exploitation strategy of the consortium including the exploitation viability of different business models.

The sections of the deliverable are presented below including the topics that they cover:

- Section 2 – Value Proposition: The objectives of the exploitation plan, presenting the overall context, scope as well as the value of the SECONOMICS framework and toolkit. The framework provides a set of methods, techniques and models to identify and evaluate risks and system concerns assisting decision-makers in the decisions to be made, evaluating economics, system, policy and societal aspects. The toolkit integrates different tools to support policy decision making in relation with the adoption of the optimal security measures according to the scenario needed.
- Section 3 – Market Analysis: The market analysis of the models and tools that can be applied by different stakeholders within the security domain to issue relevant recommendations to all actors involved with timely and relevant information and adopt proper measures.
- Section 4 – SWOT: This section presents the Strengths, Weaknesses, Opportunities and Threats of the whole SECONOMICS policy framework.
- Section 5 – Joint Business Strategy: The SECONOMICS business offering as a result of the project's activities, considering SECONOMICS as a whole. The exploitation strategy at consortium level including the IPR management and licensing.
- Section 6 – Individual Exploitation Plans: The business plans of each individual consortium partner regarding different business profiles, models and expectations.
- Section 7 - Conclusions

With respect to the methodology used in creating deliverable D9.10, the information has been collected from publically available sources (e.g. public market studies and reports, EU and national legislation, research projects, etc.) and from the interaction with the SECONOMICS consortium partners.

# 2. Value proposition

## 2.1 Current situation and capacities needed

Transportation plays a crucial role in the everyday lives of citizens and ensures the economic wellbeing of communities and countries. However public transport is open and accessible to everyone and thus susceptible to intentional disruptions and terrorist attacks. Other critical infrastructures such as power grids are also increasing concern to governments. Cyber-attacks on the electric grid systems are growing in sophistication and frequency. Such attacks come from different sources, including nation states and terrorist organizations and would result in disruption in the electrical supply system and tremendous consequences for the national economy.

To analyse how security is strengthened, two main perspectives are considered by SECONOMICS, i) how policy makers introduce new regulation and ii) how infrastructure operators ensure security.

**Policy makers**

This section is not meant to provide a comprehensive overview of the EU legislation that regulates security in infrastructures, since the application of the EU laws varies from country to country. The aim of this section is to present the core rules, actors and processes followed to introduce new regulation.

SECONOMICS places special emphasis on policy makers and regulators. The European Union is an important player in security matters where EU countries try and speak as one on global affairs. Essential authority on foreign and security policy remains with EU Member States governments, although the European Commission and the European Parliament are associated with the process. Key decisions are taken by unanimous vote. The basis for the EU’s Common Foreign and Security Policy (CFSP) includes the use of diplomacy to resolve conflicts and bring about international understanding. The principles behind these activities are known as the European Security and Defence Policy (ESDP).

The legal framework is provided by the Treaty on the Functioning of the European Union, and the Treaty on the European Union. The Lisbon Treaty introduced the appointment of an EU High Representative for Foreign Affairs and Security Policy, assisted by civilian and military staff grouped in the European External Action Service (EEAS). They are responsible for coordinating the EU institutions and the member states in order to adopt, shape and implement a common foreign and security policy.

Transport and critical infrastructure security policy is a matter of shared competence between the EU and the member states. Action should take place at the level at which it can be most effective, whether local, regional, national or EU (the subsidiarity principle). In practice, the situation differs significantly between the different types of infrastructures and transport modes, based not only on their respective characteristics, but also on the member states initiatives.

A number of measures were implemented concerning the protection of critical infrastructures at EU level such as the Proposal for a Council Directive on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection presented by the EC in December 2006 evolved into Council Directive 2008/114/EC. Protective measures against electronic attack on key computer systems (cybercrime) have been implemented through the Council Framework Decision 2005/222/JHA292 of 24 February 2005.

Currently the European Commission has presented to members a proposal to introduce several additional controls on hand luggage that can carry passengers in the plane. Two measures have been suggested: the possibility of increasing the number of prohibited items aboard and greater control of electronic devices. The fear that smart phones or tablets can hide an explosive in place of the battery has already led the United States and the United Kingdom to prevent such devices from accessing the plane if they are found to have dead batteries. Counterterrorism experts have already discussed this followed by analysis by the civil aviation.

The EU executive is also studying how to improve the recruitment and training of security guards. There are 2.5 million deployed throughout the EU, but their training and work modes are heterogeneous, causing gaps in protection. All that reflection should materialize into a new European counterterrorism strategy for next spring (2015).

**Critical infrastructure managers and operators**

Critical infrastructure managers and operators must ensure smooth operation of services within their infrastructure, which involves maximising the satisfaction of customers and employees, ensuring their safety and security, compliance with the related legislation, and meet constrained budgets.

As identified by the project SECUR-ED, the improvement of security in urban public transportation and critical infrastructures can be achieved by the operators with different measures and strategies:

- **Information management solutions**: these systems aggregate real-time information from many kinds of sources, e.g. CCTV cameras, motion detectors, access control devices and more advanced sensors and reports from front-line security personnel. These solutions provide a better awareness of the security situation and reduce the burden of personnel in security operations centres.
- **Early warning systems**: an early warning system aims to detect events that are indicators of a potential threat that human operators might miss. This solution is useful to handle large amounts of information.
- **Architecture and Interoperability solutions, communications infrastructure**: standardised architecture, interoperability solutions and good communications infrastructure increases security by leveraging the benefits of other solutions.
- **Training programmes**: training of security personnel adapted to different needs is critical.
- **Procedures**: specific risk assessment methodologies, operational and organisational procedures can be developed to improve security.

The operators will therefore consider one or several of these measures to provide a higher security standard.

## 2.2 Approach

In response to these challenges, SECONOMICS brings together a multinational team of security practitioners, economists and engineers to produce a policy toolkit that can effectively assist decision makers in identifying and reacting to public transportation and critical infrastructure threats.

SECONOMICS security scenarios include high-level and locally operational security scenarios, where the consortium first set out to identify and mitigate major security threats by exploring the implementation of coordinated solutions that could work at the European level. The project case studies successfully identified key security threats in transport (air and metro) and other critical infrastructure. In this way, the challenges of achieving pan-European security coordination have been dealt with.

The project has produced a toolkit that provides guidance to policy makers across the three industry case studies (aviation, critical power infrastructure and regional and urban transport). The workflow of the tool kit proceeds in the following general manner. First, the security domain provides qualitative and quantitative evidence on the threat actions and defensive investments that are required to mitigate threats. The SECONOMICS analyst then utilises the menu of tools to best capture the various trade-offs inherent in the security domain of interest. The models within the operationalised toolkit cover broad macro level public policy, specific regulatory interactions and finally operational adversarial analysis for individual games between attackers and defenders.

The analyst then has the ability to interrogate the existing model suites or relatively simply customise the models (by directly editing the underlying MATLAB models) and reformulate them for the particular security problem at hand. This is one of the first tools of this type and streamlines the methodological approach for a security analyst. Critically, it structures the information gathering phase and provides a framework that is complementary to existing approaches such as capability maturity analysis and conventional risk assessments.

The key objective of the models is not to be reliant on point estimates of historical data, but to allow stress testing across a range of outcomes, some of which can be characterised by scenarios.

The WP6 models are a case in point. These models utilize variations on game theory, mostly simultaneous equilibrium models, to capture domains of solutions for cost sharing and regulatory interventions in security situations. The underlying assumptions are weak. Diminishing marginal returns to security investment allow for an optimal security investment to be determined. To this, dynamic attackers are added with simply cost benefit rules. From this underlying framework, extensions and constraints such as insurance and heterogeneity in the cross section of targets (such as large and small airports, differentiated critical infrastructure) can be added.

The project has produced a general methodology for security risk models expanding and developing the methodology of Adversarial Risk Analysis (ARA). ARA extends traditional risk analysis to account for threats originated by intentional adversaries. Template models were produced which serve as backbone for building more complex and realistic models as the ones tested for the airport and urban transportation case studies. Based on them, a number of enhancements were introduced.

The more complex models were also validated with additional cases oriented towards emergent threats in cases referring to terrorism in a railway service (networks), delinquency in cities (spatial distribution) and cybersecurity. Many of the models were software prototyped to be included in the SECONOMICS Toolkit.

The general methodology is to be fed with new research on objectives, risk perceptions and attitudes, budgetary and other constraints, to finally produce the best security resource allocation for an organisation willing to protect multiple targets against multiple threats.

## 2.3 Value proposition

SECONOMICS has produced a policy framework and toolkit for planning and decision making under risk and/or uncertainty and facilitates better and more effective decision making in the security domain, minimising threats in the most cost-efficient way possible.

The policy framework combines a complete assessment of social aspects with more formal models and systems for policy-making and risk assessment.

The SECONOMICS modelling tools seamlessly transverses the social, economic and technological domains, resulting in a methodological change for decision making in the security domain.

As a result of the research activities conducted, SECONOMICS provides a set of complete and implementable critical infrastructure security policies and sheds light on the economic causes and consequences of insecurity and the impact on the perception of citizens and the direct and indirect costs of implementation. Cost calculations placed specific emphasis on increased hidden costs, decreased efficiency and trans-boundary impacts such as the interaction between security behaviour and economic growth.

The SECONOMICS Toolkit supports the following groups of stakeholders:

a) policy makers and legislators that can modify the laws and directives to adopt new security parameters. SECONOMICS will provide guidance on which types of legislative and regulatory instruments are best suited to a particular emerging security threat,
b) managers (infrastructure operators) responsible for choosing the optimal level of investment in security measures and strategies for a variety of different types of critical security domains taking into account the socioeconomic context and implications,
c) research and academic community that can continue the development and research of SECONOMICS,
d) consultancy companies from private sector that provides services to third parties and can benefit from SECONOMICS results.

These stakeholders make decisions according to the public interest at three different levels: the strategic level to set the objectives and goals to achieve; the tactical level, in which the services and security measures are set and, finally, the operational level when the services and security measures are implemented. SECONOMICS remains at a strategic and tactical level.

While the citizens are concerned on how to make more effective the security in the transport sector or in other infrastructures, they do not represent a direct target audience of SECONOMICS as they might rarely decide or push the use or adoption of SECONOMICS.

## 2.4 List of exploitable results

The SECONOMICS exploitable results include a wide range of results that complement one another and comprise the whole SECONOMICS framework. The exploitable results can be classified under five main categories:

- Best practices and methods
- Models
- Software components: SECONOMICS Toolkit (including MATLAB implementations of the models)
- Information and analysis produced during the project
- Media Corpus

The following sections list and describe the different project results for each category.

### 2.4.1 Good practice and methods

This category contains best practices to better introduce models to decision makers and techniques to conduct media analysis.

Table 1 - Exploitable result: SECONOMICS science-based practice

| | |
|---|---|
| **Exploitable result** | **SECONOMICS science-based practice** |
| **Sub-components** | - |
| **Description** | SECONOMICS "Good Practice" describes how scientific models can be introduced to and used by policy and decision makers for evidence-based policy making. This approach uses the following procedures:<br>3. Introduction and buy-in by key stakeholder: we first introduce scientific models and got buy-in by key stakeholder;<br>4. Familiarization and confidence building: we probe and explain what questions the models can or cannot answer, and what is considered by the models and what is not considered. This phase was considered essential by most stakeholders;<br>5. Calibration: we discuss with stakeholders to calibrate the parameters of the models to the particular scenarios the policymaker is interested in. We identify the parameters under the control of the policymaker and the ones defined by the environment;<br>6. What-if scenario and refinement: we analyse the scenarios to identify outcomes of possible policy decision. |
| **Exploitation strategy** | SECONOMICS science-based practice is used in each case study toolkit and in an array of research papers. Furthermore this practice will provide researchers and practitioners with information on how scientific models can be introduced and used by policy and decision makers for evidence-based policy making. The practice will be used by SECONOMICS partners in other projects in order to facilitate the communication with policy makers. |

| | |
|---|---|
| License | No licenses apply |
| Owner / Beneficiaries | ALL partners |

Table 2 - Exploitable result: Coding technique for Salience Analysis in the Media

| | |
|---|---|
| Exploitable result | **Coding technique for Salience Analysis in the Media** |
| Sub-components | - |
| Description | Innovative research methods to code and analyse in a semi-automated way media artefacts (printed and online, as well as to the analysis of social media such as blogs, forums, etc.). It is designed for three security domains: aviation, urban public transportation and CNI. |
| Exploitation strategy | This coding technique will be applied in other R&D projects. ISASCR will include this sampling technique and coding scheme into graduate courses available. Scientific output will be available to the academic community as a significant contribution to qualitative comparative methodology.<br>The technique is quite mature and can be applied with minor changes to same security domains in various countries and with some adjustments to other domains e.g., health, transport in general, oil & gas.<br>It can serve to provide consultancy services to public and private stakeholders interested in the public debate about a relevant issue.<br>Joint exploitation among partners is foreseen in order to develop and/or building of a proprietary methodology based on the media analysis. |
| License | No licenses apply |
| Owner / Beneficiaries | ISASCR, DBL, TMB |

### 2.4.2 Models

SECONOMICS has developed several models focusing on the effects of security measures. This includes models for forecasting reactions to the deployment of various security policies and deciding optimal security policies and resource allocations, mainly at the strategic and tactical levels.

They have been tested on cases in airport, metros and railway security, and cybersecurity infrastructure. Such studies may serve as blueprint to conduct further security risk analysis.

Table 3 - Exploitable result: ARA analysis for security resource allocation.

| | |
|---|---|
| **Exploitable result** | **Adversarial Risk Analysis (ARA) models for security resource allocation for protection of critical infrastructures.** |
| **Sub-components** | • ARA models to protect a single site:<br>○ simultaneous defend-attack;<br>○ sequential defend-attack;<br>○ sequential attack-defend;<br>○ sequential defend-attack-defend and<br>○ sequential defend-attack with private information models<br>○ generic interactions between an attacker and a defender<br>• ARA models to protect several sites<br>○ when they are independently located<br>○ when they are spatially related<br>○ when they are displayed as a network<br>• ARA models when there are several Defenders (single- or multi-site)<br>• ARA models when there are several Attackers "(single- or multi-site) |
| **Description** | ARA models provide optimal decisions considering protection of sites. This entails accounting for uncertainties and risk aversion of the decision maker and forecasting the actions of adversaries.<br>The models may allow developing proprietary methodologies and frameworks to guide the identification and installation of an optimal portfolio of security measures for a more effective control of aviation infrastructures and assets.<br>The models are applicable to many different types of problems in which advice can be provided to a defender that faces threats from intelligent attackers.<br>The models can also be applied to multiple sites (independent sites, networks, spatially distributed sites) however they are far more difficult to tackle than individual sites and usually entail both modelling and computational non-standard issues that need expert analysts advice, making the suitable ground for consulting activities.<br>They may deal also with cases in which there are several Defenders which, coordinated or not, have to protect from several Attackers, coordinated or not.<br>The case studies serve as blueprint for similar security case studies at the tactical level. |

| | |
|---|---|
| **Exploitation strategy** | Several of the models have been implemented with MATLAB for different use case applications and can be used with the Java interface. Therefore knowledge on these models in the form of advice on modelling risks and algorithms will be required to develop new implementations of the toolkit beyond the SECONOMICS project lifetime.<br>As a basis for future R&D projects, ARA models will be applied to energy availability risks, as well as cybersecurity, through different research activities. PhD theses are being developed by academic partners expanding the concepts in new domains. Furthermore URJC is already using ARA concepts in various courses at the Master level, replacing traditional non cooperative game theoretic concepts. Short term results (soon after the end of the project) include doctoral thesis, project proposals, post-doc positions, publications, research dissemination and grants.<br>URJC is willing to support the application of these models in partnership with consulting companies, possibly within the consortium. The ARA models can be used in a variety of applied fields beyond those included in SECONOMICS such as, to name but a few:<br>• supporting participants in auctions,<br>• supporting auction design,<br>• cybersecurity,<br>• competitive marketing,<br>• personalised marketing,<br>• national defence,<br>• social robotics,<br>• country risk modelling.<br>ARA models may be used to revisit many game theory applications in which hypothesis such as common knowledge are not tenable.<br>Beyond its academic interest, this has a large potential for consulting practice. Part of this kind of commercial exploitation will require further developments; therefore this commercialisation could be expected in 2016/17. Consulting companies could develop various products and consultancy services in the airport domain e.g. for securing sites and installations such as control towers, area control centers, runways, etc. However, many of the results may be offered already for (high level) consulting purposes.<br>Within the aerospace sector, the main potential clients and stakeholders benefiting from this result include airports, airport association, ANSP, airlines, regulators and international organisations. Some airport management organisations, such as Aerdorica and SAGA, already showed potential interest in apply and use ARA Analysis in their operational environment.<br>Great interest about the cyber-security application of the ARA models has also been showed by European Institutions and private consultancy companies working in the Aviation domain.<br>Similar sets of potential clients may be described in other sectors. |

| | |
|---|---|
| License | No licenses apply |
| Owner / Beneficiaries | Owner: URJC<br>Other Beneficiaries: AU, DBL, TMB, SNOK, Fraunhofer |

Table 4 - Exploitable result: Public Policy with mandatory and risk-based security investments

| | |
|---|---|
| Exploitable result | **Models for public policy with mandatory and risk-based security investments** |
| Sub-components | - |
| Description | The public policy and agility models of WP6 take as input the different regulatory environments, the responses and interpretation of the regulation by the CNI operator, shocks to the environment and different attacker skill level and provides the landscape of cyber security regulation for a CNI Operator. |
| Exploitation strategy | The WP6 public policy and subsidy models will be exploited by different CNI Operators such as National Grid, the transmission system operators (TSOs) across Europe and other CNI Operators, specifically in monopolistic environments where they are heavily regulated on price. Mainly it will be used by them to aid discussion with regulators at a national level and provide evidence of the trade-offs of different policy mechanisms for cyber security regulation. At a later stage the models could be used by the national regulators to help define cyber security regulation for CNI industries at a European level.<br>No business models have been explored due to the academic nature of this result. |
| License | No licenses apply |
| Owner / Beneficiaries | National Grid, University of Aberdeen, University of Durham |

Table 5 - Exploitable result: Public Policy for security investments with heterogeneous industries and network effect

| | |
|---|---|
| Exploitable result | **Models for public policy for security investments with heterogeneous industries and network effect** |

| | |
|---|---|
| **Sub-components** | WP1 deliverables<br>WP6 deliverables<br>Paper: Shim, W., Massacci, F., M., Tedeschi, A., Pollini, A. (2014) A Relative Cost-Benefit Approach for Evaluating Alternative Airport Security Policies. Paper at SecATM 2014. |
| **Description** | This analysis comprises various studies on policy and regulatory issues in aviation security by combining results from a simple quantitative economic model with a series of semi-structured interviews with key stakeholders for airport operations. In the quantitative economic analysis, we illustrate how different security strategies, policies and regulations affect industry players differently. To provide evidence elucidated in the model, we have undertaken an extensive interview process with regulators, airport managers and airport security experts. The model shows the circumstances under which the outcomes of intended security policies and regulations can be expected to differ. By explicitly considering various factors including transferable value of security training, security externalities and technological changes, the models are able to identify the discrepancy between private and social incentives.<br>The analysis shows that without appropriate setting, security policies and regulations might not produce intended outcomes. In one model, we identify that, in facilitating risk reduction in an important security setting, security training should be designed to provide security personnel with intrinsic incentives and potentially transferable values. The other study finds that without appropriate coordination, security regulation might be significantly unfair for airports with different nature. |
| **Exploitation strategy** | The results will be publicly available for download by researchers, policy makers and citizens interested to test and conduct further research on the airport security domain. In addition, the results will be used by partners in other projects.<br>Part of the models has been validated by security experts and regulators, and is ready for exploitation. Other models have finished the calibration of parameter values and toolkit implementation. After further validation, exploitation will be carried out. The exploitation will focus on supporting policy-makers in developing effective and fair regulations and policies for aviation security (e.g., effective security training strategies or fair security tax scheme). Furthermore, the results can be also be used by stakeholders in other critical infrastructure fields.<br>These models and their results could be exploited by DBL in its consultancy services for Regulators, Public Bodies and Associations of Stakeholders at European Levels, in the writing of White Papers and Reports for Policy Makers in the Civil Aviation domain and as a basis for future R&D projects.<br>The target users include Airports, Airport Association, ANSP, Airlines, Regulators and International Organisation. The European Association of Airports (ACI - Europe) already showed potential interest in apply and use the public policy models for security investments for the forecast of future trends and for supporting their analyses about security policies for |

| | |
|---|---|
| | small/medium and big airports in Europe. |
| **License** | No licenses apply |
| **Owner / Beneficiaries** | UNITN, ABDN, UDUR, DBL, AU, Fraunhofer, TMB |

Table 6 - Exploitable result: A model of contingent claims for insurance

| | |
|---|---|
| **Exploitable result** | **Model of contingent claims for insurance** |
| **Sub-components** | • D6.1 A general systems model architecture<br>• D6.4 A set of policy papers |
| **Description** | The model of contingent claims for insurance comprises game theoretic models of how groups of firms and individuals interact in the presence of security threats. This has the potential to help actuaries and consumers of insurance in determining returns on security investment and aggregate risk factors. |
| **Exploitation strategy** | This result is publicly accessible. It is mainly an academic and research result, although actuary based formulations for the insurance industry may be possible in the intermediate term (approximately 2 years) |
| **License** | No licenses apply |
| **Owner / Beneficiaries** | UNIDUR |

Table 7 - Exploitable result: Resilient risk versus rules frameworks

| | |
|---|---|
| **Exploitable result** | **Resilient risk versus rules frameworks** |
| **Sub-components** | • D1.5 Tool Validation<br>• D2.5 Evaluation tools for providers and policy paper on future and emerging threats<br>• D6.2 A report on the interaction of systems models and models of economics, law and society<br>• D6.3 Report on the Experimental Analysis<br>• D6.4 A set of policy papers |

| | |
|---|---|
| Description | The Resilient risk versus rules frameworks includes social policy models that quantify the impact of rules versus risk based policy implementations on cost and risk reduction. This is an advancement in the framework that surrounds how we create public policy institutions. |
| Exploitation strategy | This result is publicly accessible. It is mainly an academic and research result addressing policy makers and researchers in the area of public economics. Commercial exploitation could be explored in the long term. |
| License | No licenses apply |
| Owner / Beneficiaries | UNIDUR |

Table 8 - Exploitable result: A method of unifying network architecture and economic incentives

| Exploitable result | **Method of unifying network architecture and economic incentives** |
|---|---|
| Sub-components | D6.4 ‘A set of policy papers’ |
| Description | This method includes some institutional models using mechanism design approaches that provide new applied results. This innovation may provide a template for optimizing institutional structures and legal liabilities. |
| Exploitation strategy | This result is publicly accessible. It is mainly an academic and research result addressing national and supra-national policy makers. It is still a conceptual model and it is not ready for immediate commercialization/exploitation. |
| License | No licenses apply |
| Owner / Beneficiaries | UNIDUR |

Table 9 - Exploitable result: Model of Public Acceptance of Security Measures

| Exploitable result | **Model of Public Acceptance of Security Measures** |
|---|---|

| | |
|---|---|
| **Sub-components** | • D4.3 Report on Communication patterns and effective channels of communication<br>• D4.4 – Discourses and Justification of Security and Risk<br>• D4.5 Comparative quantitative analysis of security and acceptance of risk. |
| **Description** | This model explores the effects of security measures on passengers in two security domains: aviation and urban public transportation. |
| **Exploitation strategy** | This result will be made available immediately. Further academic exploitation will continue in 2015 and 2016.<br>Additional exploitation will be explored with case study partners TMB, Deep Blue and ISASCR. The findings of the model can be used to calibrate existing security procedures. |
| **License** | No licenses apply |
| **Owner / Beneficiaries** | ISASCR, TMB, Deep Blue, NGRID |

Table 10 - Exploitable result: Incentives for Security training

| **Exploitable result** | **Incentives for Security training** |
|---|---|
| **Sub-components** | • D.4.3 Report on Communication patterns and effective channels of communication<br>• D.4.4 Report on Discourses and justifications of security and risk<br>• D.4.5 Comparative quantitative analysis of security and acceptance of risk.<br>• Paper: Shim, W., Massacci, F., de Gramatica, M., Tedeschi, A., Pollini, A. (2013) |
| **Description** | This result comprises different documents and studies that incentive training of security personnel based on a model of effects of security measures on passengers in two security domains: aviation and urban public transportation. |
| **Exploitation strategy** | The results are available for download at the project website.<br>The result is still a conceptual model. It will be used for academic purposes in 2015 and 2016. Further developments might be carried out according internal strategies, to pursue commercialisation in 2016/17. |
| **License** | No licenses apply |

| | |
|---|---|
| **Owner / Beneficiaries** | ISASCR, DBL, TMB |

### 2.4.3 The SECONOMICS Toolkit (including MATLAB implementations of the models)

The project has developed a software toolkit that integrates the core models implemented in MATLAB, to support policy and decision-making to find the optimal security resource allocation. This tool allows generating infographics and communicating security complexities in a useful way.

The SECONOMICS Toolkit includes the following components:

- Underlying models: MATLAB implementations of the mathematical models (described in previous section 2.4.2) to accept certain user input
- Infographics: graphics to front the models but also ensure the context to the project case studies
- User interface and input: A user interface embedded within the infographics for the stakeholders to use.

The following figure shows the different components of the SECONOMICS Toolkit (data from different sources, Java interface, models and output) and their interactions.

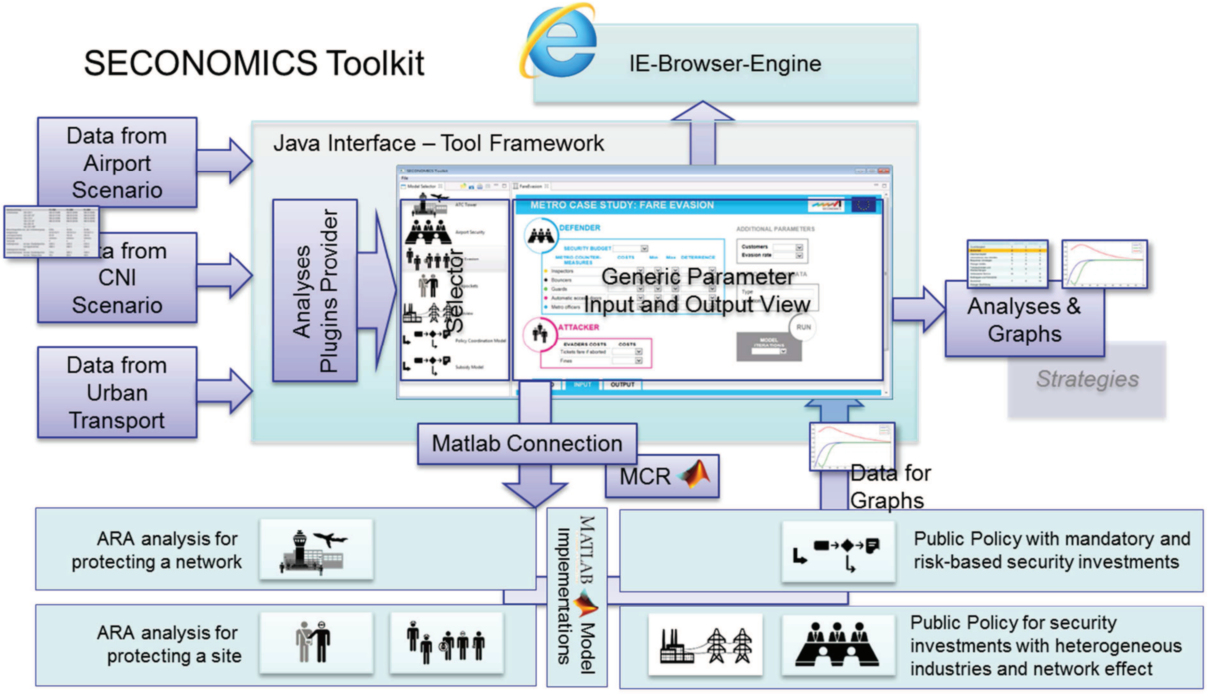
SECONOMICS Toolkit
IE-Browser-Engine
Data from Airport Scenario
Data from CNI Scenario
Data from Urban Transport
Java Interface – Tool Framework
Analyses Plugins Provider
Selector
METRO CASE STUDY: FARE EVASION
DEFENDER
ATTACKER
Generic Parameter Input and Output View
INPUT
OUTPUT
RUN
Analyses & Graphs
Strategies
Matlab Connection
MCR
Data for Graphs
MATLAB Model implementations
ARA analysis for protecting a network
ARA analysis for protecting a site
Public Policy with mandatory and risk-based security investments
Public Policy for security investments with heterogeneous industries and network effect

Figure 1 - SECONOMICS Toolkit architecture diagram

Table 11- Exploitable result: SECONOMICS Toolkit

| Exploitable result | SECONOMICS Toolkit |
|---|---|
| Sub-components | • Analyses plugins provider<br>• Selector view<br>• Parameter interface<br>• MATLAB connection<br>• MATLAB implementations of the mathematical models |
| Description | The SECONOMICS Toolkit integrates the models in different scenarios of application. It creates an easy-to-use and understandable interface with the same look and feel for all models in one tool. It provides interoperability and it is highly portable. |
| Exploitation strategy | The SECONOMICS Toolkit prototype (which is licensed as open-source) will require further developments (customization, improvement of the GUI, expert risk analysis, integration with underlying models, implementation of new templates) in order to be implemented as a commercial product and adapted for new stakeholders. Commercial activities of this product could be expected in 2017. The commercial version of the SECONOMICS Toolkit could thus be sold or licensed together with consultancy.<br>DBL is interested in commercialising the tool in collaboration with other project partners (e.g. academic partners and owners of the results) and will provide its GUI design and UX expertise, as well as aviation domain and security expertise to commercialize the product.<br>Private companies and public bodies of almost any sector can benefit of the SECONOMICS Toolkit components. The main target users belong to the civil aviation domain: airports, airport association, ANSP, airlines, regulators and international organisations as well as users belonging to the CNI domain: members of ENTSO-E, regulators<br>Further the tool platform is designed in a modular way and can so be used for other future research projects as well. |
| License | The SECONOMICS Toolkit as a whole is released under GNU Lesser General Public License (LGPL v.3.0, see http://www.gnu.org/licenses/lgpl-3.0.en.html ). It is made available at TUD's website which will be kept up to date with future improvements of the tool (including those by third parties). |
| Owner / Beneficiaries | Fraunhofer, URJC, UDUR, DBL, TMB. |

Table 12 - Exploitable result: Public Policy with mandatory and risk-based security investments

| Exploitable result | Public Policy with mandatory and risk-based security investments |
|---|---|

| | |
|---|---|
| Sub-components | - Models for public policy with mandatory and risk-based security investments |
| Description | The CNI case study toolkit based on the public policy and agility models of WP6. |
| Exploitation strategy | The toolkit is used by policy makers (the main and key client) to see details behind the toolkit, specifically the models, and speak to the lead researchers in the area to get confidence in the 'machine' behind the toolkit.<br>The envisaged users of the CNI case study toolkit are the CNI Operators (such as National Grid and the other TSOs across Europe) assisted and backed-up by the academics that developed the models. The clients of the models are the policy makers at a national and supranational level.<br>Whilst some further refinement, interpretation and industry information are required, the CNI case study toolkit will be exploited in 2015 for academic research. |
| License | No licenses apply |
| Owner / Beneficiaries | Owners: National Grid, University of Aberdeen, University of Durham |

Other models have been implemented as research and proof of concept prototypes that are not ready for immediate exploitation and thus have not been analysed in this section.

### 2.4.4 Analysis produced during the project

This category includes policy papers that have assessed media sources, European regulations, national, regional and sectorial laws and rules. They represent an opportunity to improve current regulations and promote SECONOMICS adoption in infrastructures.

Table 13 - Exploitable result: Media analysis of security perception by citizens

| | |
|---|---|
| Exploitable result | **Media analysis of security perception by citizens** |
| Sub-components | - |
| Description | This result contains a comprehensive and exhaustive analysis on the perception of security issues in the media (newspapers and blogs), complemented by surveys with end-users (i.e., passengers in the Aviation domain). |

| | |
|---|---|
| **Exploitation strategy** | The media analysis can be used immediately (i.e. in 2015) in consultancy services for airport domains and for future R&D projects, papers and reports.<br>Target users include: airports, airport Associations, ANSP, airlines, regulators and international organisations.<br>Interest has already been shown by CAA (e.g., ENAC) or regulators at EU level (Eurocontrol, DG Move, DG Airport Security).<br>The result is quite mature and developed and it can be applied already in 2015. |
| **License** | No licenses apply |
| **Owner / Beneficiaries** | Owner: ISASCR; Beneficiary: DBL, TMB |

Table 14 - Exploitable result: Recommendations on public policy for security

| **Exploitable result** | **Recommendations on public policy for security** |
|---|---|
| **Sub-components** | • D.4.3 Report on Communication patterns and effective channels of communication<br>• D.4.5 Comparative quantitative analysis of security and acceptance of risk<br>• D3.3 Urban public transport requirements |
| **Description** | Based on extensive research, the consortium provided multiple public policy recommendations for domestic and European policy making in security domain with special focus on communication and transnational European coordination. The research included the study of current and future threats on public transport in Europe, like fare evasion, pickpocketing and graffiti |
| **Exploitation strategy** | The recommendations will be made available immediately, and further academic exploitation will continue in 2015 and 2016.<br>NGRID as a CNI Operator can use the recommendations on public policy for security together with other results to understand better the regulatory landscape, the trade-offs and the aims of the different parties in more detail. From this, a CNI Operator can provide their interpretation of the landscape to liaise with their regulators. NGRID will provide their interpretation of the landscape evidenced and backed-up by the mathematics of the model and toolkit.<br>Atos will apply knowledge gained in this project in future R&D projects and services for Public Transport operators taking into account the security and its impact on societal and technical (economic) dimensions<br>Target users are the CNI operators, national and supranational policy |

| | |
|---|---|
| | makers, stakeholders, civil society groups and public transport operators. |
| **License** | No licenses apply |
| **Owner / Beneficiaries** | ISASCR, National Grid, University of Aberdeen, University of Durham, Atos, TMB |

### 2.4.5 Media Corpus

Table 15 - Exploitable result: SECONOMICS Media Corpus

| | |
|---|---|
| **Exploitable result** | **SECONOMICS Media Corpus** |
| **Sub-components** | D.4.4 Report on Discourses and justifications of security and risk<br>D.4.5 Comparative quantitative analysis of security and acceptance of risk |
| **Description** | The SECONOMICS media corpus includes a collection of over 2800 relevant articles on three security issues: CCTV, 3D body scanner and Stuxnet, in 10 national languages, over period of 40 months (2010/2013). |
| **Exploitation strategy** | Media Corpus can be utilized for further in-depth exploitation of the selected security issues, especially for academic purposes. |
| **License** | No licenses apply |
| **Owner / Beneficiaries** | ISASCR |

## 2.5 Matrix of exploitable results and stakeholders

The following table shows the most important group of stakeholders for each exploitable result.

Table 16 - Matrix of results and target stakeholders

| | Academic and research | Policy makers | Consulting companies | Infrastructure operators |
|---|---|---|---|---|
| SECONOMICS Science-based Practice | X | X | | |

| | Academic and research | Policy makers | Consulting companies | Infrastructure operators |
|---|---|---|---|---|
| Coding technique for Salience Analysis in the Media | X | X | X | |
| ARA analysis for protecting sites | X | X | X | X |
| Public Policy with mandatory and risk-based security investments | X | X | | X |
| Public Policy for security investments with heterogeneous industries and network effect | X | X | | X |
| A model of contingent claims for insurance. | X | | X | |
| Resilient risk versus rules frameworks. | X | X | | |
| A method of unifying network architecture and economic incentives. | X | X | | |
| Model of Public Acceptance of Security Measures | X | | | |
| Incentives for Security training | X | | | |
| Public Policy with mandatory and risk-based security investments | | X | | X |
| The SECONOMICS Toolkit | X | X | X | X |
| Media analysis of security perception by citizens | X | X | X | X |
| Recommendations on public policy for security | X | X | X | X |
| SECONOMICS Media Corpus | X | | | |

# 3 Market analysis

This section provides insight into the market environment, economic and industry trends, size of the market and market segments, with the objective to assess opportunities in a competitive market.

## 3.1 Market information, trends, barriers and potential for 2020

### 3.1.1 Global transportation security and infrastructure investment

The forecast for the global transportation safety and security market is positive. Among others, two studies suggest this trend:

- BCC Research studied the market for transportation security and predicted that the value of the global market would reach $5.9 billion in 2015 after increasing at a five-year compound annual growth rate (CAGR) of 20.4%.
- RESEARCH AND MARKETS forecast that the global transportation safety and security market will grow from $37.80 billion in 2013 to $62.96 billion in 2018, at a CAGR of 10.7% from 2013 to 2018.

The number of passenger traffic and freight movement across the globe has increased, and with it the demand for technology-driven, automated, and highly secure transportation has grown immensely, reports RESEARCH AND MARKETS. Increased crime, accidents, antisocial behaviour, and continuous attacks[1] have forced governments to spend a huge amount on transportation safety and security needs by providing high-tech integrated systems and services.

Transportation security practices will continue to mature and adapt to a dynamic context, the complexity of technology, increased operations and globalization, as there is a need to apply modern security practices. A new generation of transportation security equipment has or will soon be introduced, driven by changing security needs and threats and by technological innovations that improve threat detection. Each time a change is introduced, new training for security personnel and new regulatory approach is required. The education approach has to be structurally cost-efficient, integrated and innovative.

Consulting and system integration services are one of the biggest revenue contributors in the transportation safety and transportation security services. BCC Research considered that the security transportation market can be broken down by technology into five segments and provided the following estimations for each global market value:

- **The video surveillance** segment: it is expected to reach a value of $1.9 billion in 2015.
- **The biometrics** segment: it should be worth nearly $3 billion in 2015.
- **The access control technologies** segment: in 2015 it should be worth $626 million.

[1] In 2014, there have been high profile attacks on aviation infrastructure in Pakistan. The months of June and July, 2014 have witnessed significant tightening of security procedures at airports in the USA and Europe in response to a significant terror warning that explosive devices were being constructed to by-pass current airport security measures.

- **The CBRN** (chemical, biological, radiological, nuclear) detection segment: it should amount to $356 million in 2015.
- **The perimeter intrusion detection technologies** segment: it should be worth $55 million in 2015

Figure 2 shows the evolution in the relative share of each technology segment.

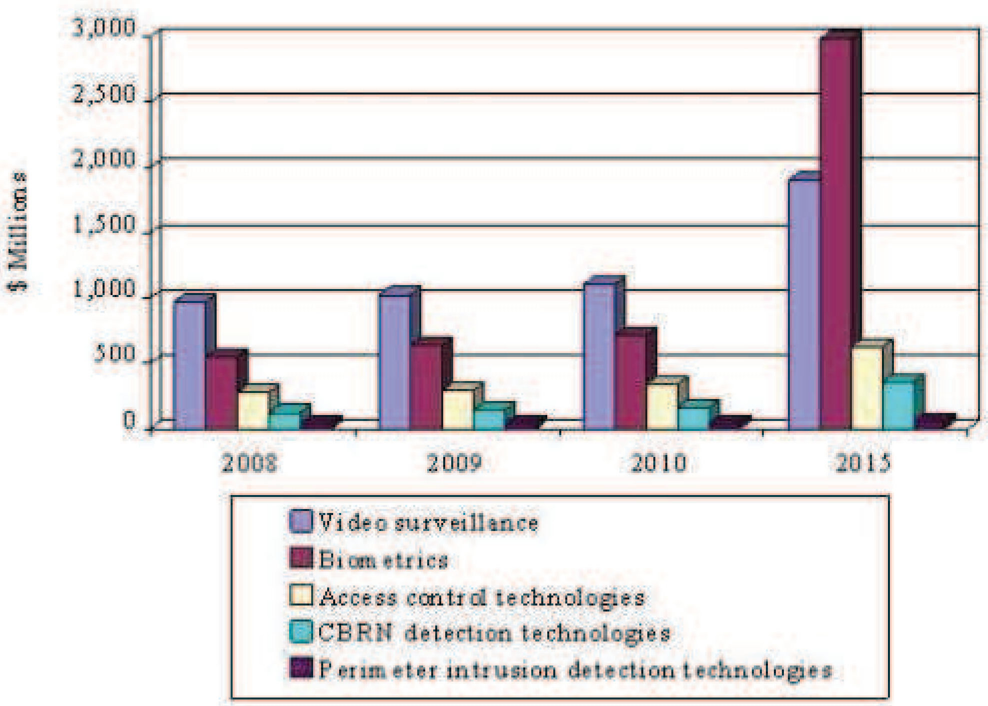

Figure 2 - Global security solutions for the transportation market by technologies, 2008-2015 ($ millions, source: BCC Research)

It is worth noting the significant development of the biometric technologies together with video surveillance.

MARKETS AND MARKETS forecasts that North America is expected to be the biggest contributor in terms of revenue contribution, while the growing markets Asia Pacific, Middle East and Africa and Latin America, are expected to experience increased market traction with high CAGR's, during the forecast period (2013-2018).

Asia Pacific, Middle East and Africa are expected to be the lucrative markets in the coming years. These regions are growing due to raise in infrastructural development of critical transportation facilities; also, governments are spending huge amount on air, water, and land safety and security-related projects.

#### 3.1.1.1 Urban train systems

Mass transit systems are at the core of public transportation in cities of different sizes around the world. According to UITP's statistics, 148 cities have a metro system and there are close to 540 lines in total. Together, they carry over 150 million passengers per day. Two-thirds of the world's metro systems are located in Asia and Europe (50 and 45 respectively). There are 16 systems in Eurasia, 16 in Latin America, 15 in North America and 6 in the Middle East and North Africa (MENA) region. The networks of Paris and London are ranked 9th and 11th respectively as the busiest metro systems in the world.

The number of cities with metros continues to grow and the increase has actually accelerated. From the 1970s to the year 2000, there were approximately 25 new systems every decade. Since the start of the new millennium, more than 45 cities have been added to the list.

In parallel to the increase in the number of metro networks, many cities have expanded their network. Today there are 9,000 metro stations in the world and 11,000 kilometres of line infrastructure. Average line length is approximately 20 kilometres. London, Madrid and Paris are ranked 3rd, 8th and 10th respectively among the world longest networks. Europe has the highest network density with an average inter-station distance of approximately 1 kilometre.

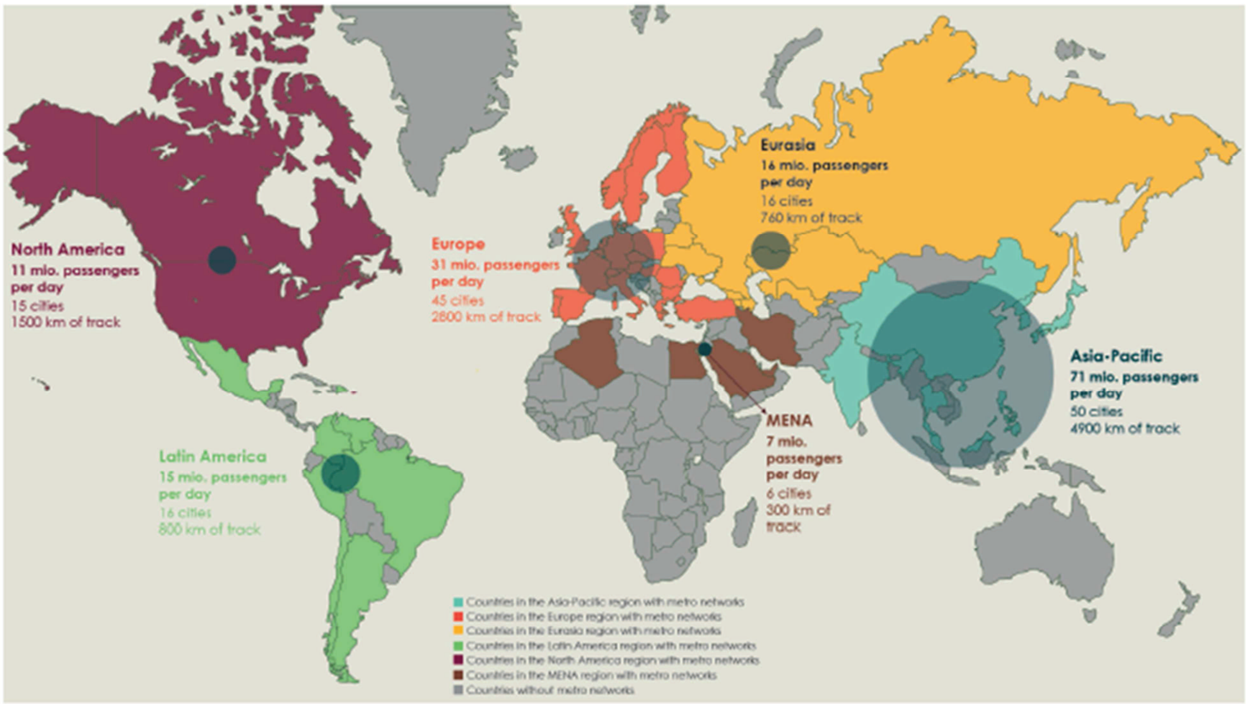
Eurasia
16 mio. passengers
per day
16 cities
760 km of track
North America
11 mio. passengers
per day
15 cities
1500 km of track
Europe
31 mio. passengers
per day
45 cities
2800 km of track
Asia-Pacific
71 mio. passengers
per day
50 cities
4900 km of track
MENA
7 mio.
passengers
per day
6 cities
300 km of
track
Latin America
15 mio. passengers
per day
16 cities
800 km of track
🟦 Countries in the Asia-Pacific region with metro networks
🟥 Countries in the Europe region with metro networks
🟧 Countries in the Eurasia region with metro networks
🟩 Countries in the Latin America region with metro networks
🟪 Countries in the North America region with metro networks
🟫 Countries in the MENA region with metro networks
⬜ Countries without metro networks

Figure 3 Map of countries which have metro networks, according to world region, with average daily ridership. The number of cities in each region with metros and total length of metro infrastructure are also shown. The size of the bubbles reflects ridership figures (source: uitp.org).

The project SECUR-ED identified the main directions and trends in urban transportation security:

- Awareness about the current cyber threats in public transportation systems is not sufficiently widespread, making awareness programmes for transport operators an urgent necessity. Awareness is needed at Management, Operations and Suppliers levels.
- The particular nature of potential threats combining security, safety and cyber security very specific to a transport operator is still an impediment for cooperation between departments.

- Development of a holistic risk assessment/management view for each transport operator is required to drive radical changes and provide foundations to bring new skills needed to overcome cybersecurity threats
- Due to the highly heterogeneous nature of technologies in use within a transport operator, there are several security frameworks, standards and guidelines that may be applicable to different parts of the transport operator infrastructure, allowing the transport operator to give the first steps on implementing a cybersecurity program. Nevertheless, those standards often overlap, contradict or leave gaps and were not designed in a holistic way having the public transportation business and its unique combination of threats in mind
- Several national authorities consider that regulation is of utmost importance to guarantee the security of European public transportation. EU experts (DG CNECT) already recommend that regulations address mandatory cybersecurity standards, certifications and guidelines for critical infrastructures including public transports, with mandatory periodic auditing and security testing, as well as incorporation of cybersecurity supervision capacities in existing local supervision bodies.
- To assess, monitor and compare the implementation of measures by transport operators and member states, a common generic measurement tool (i.e. a cybersecurity capability maturity model that covers technology, regulatory, educational and operational dimensions) will need to be developed.
- To support transport operators, further development of new technologies affiliated to cyber resilience is required to face the continuous increase of attacks and the specific nature of pre-defined data flows in many instances of industrial and, transport and energy automation systems.

Transport Canada considers that transportation operators are advancing their own security culture and are adopting security measures as a matter of good business, rather than because they are imposed by regulatory requirements.

#### 3.1.1.2 Aviation

A distinction can be made between urban train transport and aviation in terms of number of passengers and the intrinsic open and accessible nature of the aviation environment. Therefore security measures cannot be copied and pasted from one environment to another.

The airport security market has been resilient against financial worries as security in aviation remains a priority for governments. The sector will continue to show strong growth with the largest increases at airports with greater passenger and cargo volumes. Visiongain has determined that the value of the world aviation security market reached US$19.48bn in 2014. This sector will be driven by the continuing need for authorities, regulatory bodies and operators to ensure that the necessary security measures are implemented to detect and mitigate evolving threats to the air transport industry.

At global level, emerging economies in Asia and Latin America are expected to grow at a faster rate than long-standing industrialized economies such as those in Canada, the U.S. and Europe. Aggressive airport infrastructure projects in India and China will drive airport security markets to show the greatest growth. China is planning to build 45 new airports by 2017 and to expand existing facilities.

Frost & Sullivan identified the following market challenges to improve airport security: cost, privacy and other legal issues, lack of staff diligence, lack of training, disconcerted efforts, faulty/obsolete equipment and propaganda.

Security costs represent up to 35% of overall airport operating costs (European Commission, 2009). The impact of cost of the adoption of security measures was well exemplified when the New Zealand government rejected in 2009 a proposal to screen all passengers and their baggage on internal flights, saying that the cost of such measure would cost US$ 94.4 million over 10 years, and would create costs for airports, airlines, government and ultimately passengers. Instead, other measures were adopted such as the strengthening of existing cockpit doors and others.

Several key trends in airport security solutions can be highlighted:

- Security in the aviation sector has advanced with the application of new technologies, coupled with evolution in training and heightened use of threat-risk analyses to identify priority areas.
- Operational efficiency and reduced costs will drive airport operators to invest in security technologies
- The dynamics of the market will slowly shift away from labour-intensive activities to an increasingly technological approach as end users look for more operational efficiencies and cost savings
- Integration of security systems throughout airports will continue to be a key requirement and investment for airport security operators to facilitate this technological change.
- Growth in IT connectivity throughout the airport will increase cyber security expenditure in the market to ensure that systems, both security and operational, are fully protected.
- There is a continued preference for operationally proven technologies as opposed to new concepts.
- Competition in the market segments remains strong with a number of different security companies competing on upgrades and new contracts. It is a difficult market to enter if one is not already well-positioned.
- Legislation will be renewed for all air transportation industry stakeholders and regulatory bodies will continue to heavily influence market changes, security requirements, and consequently, security investment.
- Security Authorities and other service providers will work closely with industry to understand and minimize the regulatory burden while promoting further harmonization of the regulations with international standards.

### 3.1.2 Power grid infrastructures

As with the transportation sector, two aspects can be considered to study the evolution of the power grid security market: plans for new infrastructure and vulnerability to new threats (e.g. cybercrime).

### New infrastructure

The forecast for the energy (electricity and gas) sector is positive as new investments in infrastructure are required over the next years. According to the German Institute for Economic Research, until 2030 about 2500 billion euro will have to be invested in the European energy sector; this corresponds to an annual investment requirement of almost 150 billion euro per year. The investment requirements in the electricity sector are estimated to be at least 70 billion euro per year, two thirds of which are for electricity generation and one third for the electricity network. In addition, investment expenditures of about the same order of magnitude of 70 billion euro will have to be covered for energy efficiency measures.

In the natural gas transmission infrastructure there will be additional investment requirements in order to ensure diversification and security of supplies to the EU member states. It will be hard to expand domestic natural gas extraction but creation of infrastructure to import natural gas to Europe via pipelines or liquefied natural gas terminals and the improvement of interconnection within Europe is required

The appropriate regulatory framework is needed to ensure that investments are carried out at the national and European levels. In particular cross-border investments are still problematic. Multinational and Europe-wide cooperation is needed to advance the market integration and warrant that the positive effects of infrastructure investments can be harvested. The European Union has a prominent role to play beyond providing funding support, in particular in the energy corridor planning. Moreover, the project bonds by the European Investment Bank may be a suitable instrument to support sustainable energy infrastructure investments in Europe at large scale.

### Cyber-security

Cyber-attacks against vital energy infrastructure are growing. The US National Security Agency believes that electricity grids top the cyber target list for terrorists. The list of main recent attacks includes:

- Hundreds of energy companies across the US and Western Europe reported infiltrations in their computer systems by collectives of hackers in 2013.
- In May 2014, the US Department of Homeland Security revealed that an “advanced hacking group” had compromised the control network of an unidentified public utility.
- A month later, the US traced dozens of hacking attempts on utilities and gas pipelines in 2012-13 to the Chinese army.

Maurice Adriaensen, the head of DNV GL’s department of operational excellence declared that the majority of cyber incidents in the past year in the U.S. occurred on energy infrastructure. Adriaensen also reported some incidents in the renewable and wind industry in particular, which is already aware of the threats.

In Europe, countries have responded to the threat by establishing national cyber security centres to monitor their critical infrastructure. But it is the power utilities that ultimately will have to pay for the enhanced security, at a time when they are also facing grid challenges and, in many places, a fall in income due to the rise of distributed renewables.

According to a study by Ernst & Young each power and utility company is spending more than $3m a year on information security, including protection from cyber threats. Market researchers at the International Data Corporation estimate that consulting and testing services associated with cyber security for European utilities will more than double by 2016, to be worth €412m ($564m) a year.

SECONOMICS deliverable D2.5 'Evaluation tools for providers and policy paper on future and emerging threats' presents specific threats and avenues of concern in the future that are listed below:

- Predominant threats come from nation states. There are a lot of threats from adversarial nation states potentially taking control of Energy Companies they may want to bring down at some point in the future. Another possible threat is the insider threat. There are also threats from activists and hacktivists.
- Threats can come also from informal procurement. CNI Operators can buy something that is already infected, from a cyber-perspective, as there is often a false sense that the vendor has taken the adequate steps to protect their product. However, the product can have exploitable vulnerabilities within it.
- There are threats around the life cycle management. Engineers used to install things (OT equipment) on their own accord for the last 40 years. Now, OT equipment that is being installed within CNI Operators has not got a life cycle and reliable inventories are not being kept. With OT equipment now including a significant amount of IT, there will be unpatched IT assets in the core CNI environment.
- There are an increasing number of viruses and malware out in the wild. Even if they are not targeting the energy sector, they could take out the energy sector because the vulnerabilities they exploit are not sector specific.
- Connectivity - Every company wants more and more data and they are connected to more and more company systems. They are opening more doors than they are closing.
- More holistically, we are much more dependent on the internet now, but at the same time this causes the greatest threat. CNI is dependent on the internet as well, not just citizens. All this exposure to the internet is attractive to people who want to exploit it for their own (malicious) purposes. A circle of hacktivists, criminals and, at the other the end of the scale, nation states could have this intention.

## 3.2 Stakeholders analysis

This sections aims to identify the main players involved in the future use of SECONOMIC results and services according to stakeholder segment. As already stated, SECONOMICS targets four main groups of stakeholders: policy makers, infrastructure managers and operators, research and academic community, and consultancy firms.

### 3.2.1 Policy makers

Policy makers and regulators at different levels (European, national, regional and local) are required to decide the countermeasures for high-level security scenarios. Examples of high-level scenarios are passenger and luggage security checks or airport personnel training program. Governments at all levels may be interested in the SECONOMICS outcomes (at the strategic-tactical level) to predict security incidents and propose a potential alternative to, in some cases, save lives. Based on the SECONOMICS recommendations, policy guidance could be provided for the implementation of optimal calibrated regulation and regulation structures. Helpful insight might be provided to decide which aspect of security should be driven by legal regulatory instruments, and which should be driven by more agile industry agreed standards, what are the correct standards of security, etc…

There are a number of stakeholder groups involving the transport and critical infrastructure security. The distinctions between them depend on the decisions they can make and how those decisions affect other groups. In generic sense, there are three large stakeholder groups: the regulatory making groups who can decide on high level policies and regulations, the infrastructure operation groups who can make low level operation decisions, and the end user groups who can make individual decisions. They are different in motivations and sometimes benefits in making decisions. Some stakeholders may belong to more than one group.

In the case of urban public transport, usually the applied security regulations are defined at local level. City policy makers decide how to deal with security issues in public transport, even though some national and European level coordination also is given.

At international level the International Civil Aviation Organization (ICAO) works together with nation states and key industry organizations to develop policies and standards with aviation security provisions. Responsibilities include:

- Regulate general security requirements for airside and airport perimeter (fences, walls, intrusion detection system, CCTV system, security lighting and patrols by guard forces.)
- Regulate screening requirements for staff before granted access to security restricted areas.

As regards to Pan-European coordination for security threats, some initiatives exist at European level. One of the most important and essential is the coordination between law enforcement agencies, as it was reported by the police representatives during the Barcelona validation workshop. So, at this level, the current coordination initiatives present in Europe are the following:

- **Interpol:** Not restricted to the European scope, but widely used by police in Europe. It basically facilitates international police cooperation, by providing information request services among police bodies for investigation purposes. This is essential to facilitate investigation on criminal organizations that operate transnationally and beyond the EU borders.
- **Schengen Information System (SIS):** This system, managed by the Home Affairs DG of the European Union, is the largest information system for public security in Europe, and is an intergovernmental initiative under the Schengen Convention.

This system holds information and alerts on individuals, as well as information on items such as motor vehicles, firearms, identity documents and others. The information is entered into the system by national authorities and forwarded via the Central System to all Schengen States. The uses of this system are for national security, border control and law enforcement purposes.

- **Europol:** It is the European Union's law enforcement agency whose main goal is to help achieve a safer Europe for the benefit of all EU citizens. Europol is a hub for criminal information and a centre for law enforcement expertise. The agency has a large analytical capability providing strategic and forward-looking analysis of crime and terrorism in the European Union.
- **The European Aviation Safety Agency** (EASA): EASA addresses ICAO standards and goes beyond them to increases safety and security of aviation in Europe region. EASA's responsibilities include the following tasks:
    - Regulate national aviation security program (NSP) requirements with commitment that every air carrier and airport operator, handlers and service providers to have security programs.
    - Impose one-stop security requirement within Europe.
    - Allow member states to adopt alternative security measures with adequate level of protection on the basis of local risk assessment at airports with specific characteristics.
    - Regulate security examination methods: screening methods (x-ray, hand search, visual check etc.,), supplementary means of examination, and security control of supplies sold or used in security-restricted areas.
    - Impose security requirements for the air navigation services (ANS), air traffic management (ATM), communication, navigation and surveillance (CNS) assets and personnel.
- **EUROCONTROL** is the European Organisation for the Safety of Air Navigation. Founded in 1960, it is an international organisation working for seamless, pan-European air traffic management. EUROCONTROL is a civil organisation and currently has 41 member states
- **The European Union Agency for Network and Information Security** (ENISA) is an agency of the European Union that supports pan-European cybersecurity exercises. ENISA assists the Commission and the Member States in meeting the requirements of network and information security, including present and future EU legislation.
- **The European Network of Transmission System Operators** (ENTSO-E) represents 41 electricity transmission system operators across Europe. ENTSO-E promotes closer cooperation across Europe's TSOs to support the implementation of EU energy policy and achieve Europe's energy & climate policy objectives. ENTSOE has a number of groups that are working to protect the critical assets of the electricity transmission networks
    - Critical Systems Protection (CSP). The CSP working group is made up of the cyber security experts from each TSO who discuss and put together papers that can enter the standards and law of network operations across Europe.
    - Electronic Highway Working Group (EHWG)

  - Cyber Security Special Interest Group (CSSIG)
- Various **Directorate Generals of the European Commission** have recently created working groups or task forces, or have consulted experts in order to identify recommendations to better fight against terrorism and other major threats in Europe. A forum has been created in 2007, called European Security Research & Innovation Forum (ESRIF), which developed a European Security Research & Innovation Agenda (ESRIA) 277. The Directorate-General for Mobility and Transport (DG MOVE) is a Directorate-General of the European Commission responsible for transport within the European Union.

At national level, each country has one civil aviation authority to overlook all of its aviation issues, including aviation security. In addition to complying with the requirements from ICAO and EASA, the national regulators impose more detail or additional requirements.

Key stakeholders responsible with security topics at national level have been identified among the countries of consortium:

## Germany

The German security authorities are the following:

- **Federal Minister of the Interior** (Bundesminister des Inneren) for nation-wide affairs and international cooperation;
- **The Federal Minister for Transport, Building and Urban Development** is in charge of ensuring that the federal legislation is applied in the respective sectors. The Transport Ministry is responsible for the operational laws and regulations in respect to operating a transport company.

## Italy

The effective measures and actions are entrusted to the *Ministeries of Interior, Defence and Justice*. In addition, there are also the following intelligence services:

- **the Intelligence and Security Department** (Dipartimento informazioni per la sicurezza);
- **the Foreign Intelligence and Security Agency** (Agenzia informazioni e sicurezza esterna) ;
- **the Internal Intelligence and Security Agency** (Agenzia informazioni e sicurezza interna).

**The Italian Civil Aviation Authority** (ENAC) is the National Authority committed to oversee the technical regulation, the surveillance and the control in the civil aviation field. ENAC is engaged in dealing with the diverse regulatory aspects of air transport system and performs monitoring functions related to the enforcement of the adopted rules. ENAC's responsibilities include the control of the land-side safeguard of passengers, on board aircraft, inside and outside the airports, aimed at the prevention of illicit acts.

## Spain

The Spanish entities responsible with security topics are spread across national and regional levels. The national level is represented through the **Ministry of Interior** (Ministerio del Interior) and **Civil Defence National Commission** (Comisión Nacional de

Protección Civil). **The Spanish Aviation Safety and Security Agency** (AESA) ensures that civil aviation standards are observed in all aeronautical activity in Spain. Among other competences it is in charge of oversight, inspection and planning of airport security and has authority to impose penalties for breaches of civil aviation standards.

The regional level involves the regional autonomous governments. As far as Video-Surveillance is concerned, other entities have been created: **the Commissions for the Safeguarding of Video Surveillance**. **The Ministry of Transport** is also involved in the case of transport security. Other ministries that may be involved are: **the Ministry of Communications and the Ministry of Defence**.

## Turkey

The ministries responsible for implementing and overseeing security measures are the **Ministry of Defence, the Ministry of Interior, the Ministry of Justice and the Ministry of Transport and Communication** is also involved concerning public transport.

## Norway

The authorities in charge of dealing with security-related topics are the **ministry of Home Affairs, the Ministry of Justice, the Ministry of Defence, the Ministry of Foreign Affairs and the Ministry of Transport and Communications. The National Security Authority** (Nasjonal sikkerhetsmyndighet) is a security agency (directorate), acting under the Ministry of Defense (but also reporting to Ministry of Justice and the Police in civilian matters). It is responsible for preventative national security, ICT security matters, identifying national objectives of special interest and reducing vulnerability to internal and external threats. It works on national level, alone and in cooperation with the Police Security Agency and Norwegian Intelligence Service, and the Directorate for Civil Protection and Emergency Planning

## United Kingdom

Key security-related authorities include the following entities

- **Centre for the Protection of National Infrastructure** (CPNI) is the United Kingdom government authority which provides protective security advice to businesses and organisations across the national infrastructure.
- **The Civil Aviation Authority** (CAA) is the independent aviation regulator in the UK, which oversees and regulates all aspects of civil aviation including safety regulation and consumer protection.
- The rail sector is regulated by the **Office of Rail Regulation** (ORR), but the Government is a direct and active stakeholder with extensive involvement in setting detailed policy and strategic direction. In rail, the Government directly specifies many of the investments in the rail infrastructure.
- **The Department for Energy and Climate Change** (DECC) is responsible for ensuring the security of supply of energy i.e. there is enough electricity generation capability for the long term future of the UK. This includes power generation, energy transmission, energy distribution and supply to the 'last mile'. DECC identifies and assesses risks to energy assets and networks including from terrorism, cyber-attack, international military crises, and natural hazards and major accidents. DECC is led by a government minister.

## Czech Republic

The Czech security authorities are the following:

- **Ministry of Interior** of the Czech Republic is supreme office for the realms of public administration, internal security, border protection and eGovernment in the Czech Republic.
- **Ministry of transport of the Czech republic**
    - Ensures the preparation, creation, and monitoring of the Czech Transportation Policy, including strategic and conceptual documents for the Ministry;
    - Elaborates documents concerning the development of transportation networks in the Czech Republic, and documents concerning the use of innovative technologies in transportation; formulates transportation prognoses;
    - Elaborates proposals of priorities for the construction of transportation networks, based on their economic efficiency, risk, and benefit analysis;
- **Air Accidents Investigation Institute** (AAII). The AAII´s primary task in civil aviation is investigation into air accidents and serious air incidents. Other important tasks include the gathering, processing and evaluating information on occurrences in civil aviation. In addition, AAII participates in meeting requirements in civil aviation safety resulting from the Czech Republic membership in the EU, ICAO, ECAC and EUROCONTROL. It also takes part in forming safety policy of civil aviation, formulating laws and implementing legislation, and preparation of bills and regulations.

Local decision makers in the transport sector include air national service provider ANSP, airport operators, security operators, airport service operators and public services connecting to the airport. Since many requirements from high level regulatory bodies are general and instructive, it is up to each local entity to decide proper security measures. For example, the US Transportation Security Administration (TSA) only sets minimal security standards at airports and provides some training to outside security officers from these state and local authorities[2]. Thus, the decision makers at each airport need to decide on proper security countermeasures.

Specifically concerning **cybersecurity**, as described by the TENACE project, several organisations are involved at EU level:

- In the Network and Information Security (NIS) area, **the European Network and Information Security Agency (ENISA)**, established in 2004, is responsible for improving network and information security. Currently a new regulation to strengthen ENISA and modernize its mandate is under examination by the Council of Europe and the European Parliament. ENISA will also be responsible for building

[2] http://www.huffingtonpost.com/2012/06/06/airport-security-terrorism_n_1573623.html

expertise in security of industrial control systems, transport and energy infrastructure.

- **A Computer Emergency Response Team at EU level (CERT-EU)**, responsible for the security of the IT systems of EU agencies and institutions, was established in 2012.
- Furthermore, in March 2009, the European Commission established **the European Public-Private Partnership for Resilience (EP3R)** with the objective of encouraging sharing of NIS related information between interested parties in the public and private sector at European level.
- In the area of law enforcement, in 2013, **the European Cyber Crime Centre (EC3)** was formed within Europol to represent the European focal point of the fight against cybercrime. In particular, EC3 will provide analysis and intelligence, support investigations, provide high level forensics and facilitate cooperation and information sharing between the competent authorities of member states, the private sector and other stakeholders. Europol/EC3 and Eurojust will cooperate closely to improve their capability in fighting cybercrime.
- In the area of defence, the main responsibility for cyber defense at EU level is the **European Defence Agency (EDA)**. The European strategy for cybersecurity supports cooperation and information sharing between these organizations, in particular ENISA, Europol/EC3 and EDA, and between these and their counterparts at national level.
- The European Commission and the member states engage in dialogue with global partners and organizations such as the Council of Europe, OECD, OSCE, NATO and UN. ENISA provides a list of national cybersecurity strategies through its website

### 3.2.2 Infrastructure managers and operators

The infrastructure managers are the owners and operators of the different national infrastructures (rail, airports, power grid, etc…). They must ensure safe and effective management and development of that infrastructure. As the owners and managers of the infrastructure they decide how it is run and maintained, however they operate under a licence enforced by the regulatory entities which contains conditions with which they must comply.

**Urban train**

The main urban train system operators among the countries of the consortium are the following:

- Germany: Berlin U-Bahn and S-Bahn, Frankfurt U-Bahn and S-Bahn, Munich U-Bahn, Hamburg U-Bahn and S-Bahn, Nuremberg U-Bahn
- Italy: Brescia Metro, Milan Metro, Rome metro, Catania Metro, Genoa Metro, Naples Metro, Turin Metro
- Spain: Barcelona Metro, Madrid Metro, Metro Málaga, Bilbao Metro, Metro Valencia, Metro Sevilla
- Norway: Oslo Metro
- United Kingdom: London's Crossrail, London Underground, Glasgow Subway, Docklands Light Railway, Tyne & Wear Metro

- Czech Republic: Prague Metro
- Turkey: Adana Metro, Ankara Metro, Bursaray, Istanbul Metro, İzmir Metro

**Aviation**

**Airports Council International (ACI)** is the only global trade representative of the world's airports. Established in 1991, ACI represents airports' interests with governments and international organizations, develops standards, policies and recommended practices for airports, and provides information and training opportunities to raise standards around the world. It aims to provide the public with a safe, secure, efficient and environmentally responsible air transport system. The list of main airport operators can be found at https://www.aci-europe.org/membership/members-list.html

**The Civil Air Navigation Services Organisation (CANSO)** is the global voice of the companies that provide air traffic control, and represents the interests of **Air Navigation Service Providers (ANSPs)** worldwide. The list of European ANSPs can be found at https://www.canso.org/canso-members?field_regions_tid=23&field_membership_type_tid=All

**The International Air Transport Association** (IATA) is the trade association for the world's airlines, representing some 250 airlines or 84% of total air traffic. IATA supports many areas of aviation activity and helps formulate industry policy on critical aviation issues. IATA's strategy includes assessment of the threats and risk of cyber-attack, advocacy for appropriate regulation and mechanisms for increased cooperation throughout the industry and with Governments. In 2014 IATA published a toolkit to assist airlines in understanding and better defining the risks to their organizations. This includes a situational assessment of cyber security in the industry, an introduction to cyber threats, a framework for assessing risk, and guidance material for setting up a cyber-security management system. A program is also planned to assist airlines to test the new toolkit.

**Electricity transmission operators (TSOs)**

Within the different components of electricity delivery SECONOMICS focusses on electricity transmission (other components are generation and distribution). Many nations within the EU have large private organisations that own and operate the Electricity Transmission networks in those countries. The list of the main European **TSOs** can be found at https://www.entsoe.eu/about-entso-e/inside-entso-e/member-companies/Pages/default.aspx. The association of Europe's TSOs for electricity is called the **European Network of Transmission System Operators for Electricity** (ENTSO-E).

### 3.2.3 Private sector, industry, consultancy companies

Industry and consultancy firms provide infrastructure operators with assessment, analysis services and protection and detection equipment. Innovative technologies offered include tomography detection, secure communication system, intelligent avionics systems, real-time video surveillance solutions, and threat image protection.
This segment will be interested in SECONOMICS results in a variety of ways:

- Use and adjustment of project results (methods and tools) in standard development projects within industry partners to improve existing and new products to be capable for better developing secure large and complex composed services. This potentially includes collaboration of project partners on further methods and tools development. The experiences of developing tools and policy instruments will result in positive externalities for partner institutions and the wider community.

- Exchange of experience and knowledge in different business environments through case studies execution using the SECONOMICS techniques.
- The support tool designed. Initially adaptable to three use cases: Grid, transport and airport. This support tool could be adapted to new use cases.

By way of example the following list shows some of the leading transport and infrastructure security companies.

- THALES: it offers a portfolio of security solutions for airports and port infrastructures. Solutions include assessments and equipment e.g. for access control points and network cameras. URL: https://www.thalesgroup.com/en/worldwide/security/what-we-do/critical-infrastructure/airports-ports
- Selex ES: it provides airport operators with specific security systems or turnkey solutions that assimilate data from video surveillance, access control, anti-intrusion devices and cyber security to provide an operational picture. URL: http://www.selex-es.com/domains/smart/transport/airport-solutions/airport-security
- INDRA: INDRA develops open and stand-alone solutions for management and secure control of the airport scenario. Products include perimeter protection, perimeter CCTV and mobile indoor camera support, smart video, surface radars and buried unattended sensors, biometric mechanisms, fire detection, frequency inhibitors, video analysis (abandoned objects and suspicious behaviour). URL: http://www.indracompany.com/en/sector/airports/offering/security
- American Science and Engineering. URL: http://as-e.com/products-solutions/markets/critical-infrastructure-high-threat-facilities
- Analogic Corporation: among other solutions, Analogic develops automated threat detection for aviation security. URL: http://www.analogic.com/solutions-security-checkpoint.htm
- G4S is a British multinational security services company. It is the world's largest security company measured by revenues and has operations in around 125 countries, with over 620,000 employees. URL: http://www.g4s.com/en/What%20we%20do/Sectors/
- Human Recognition Systems: HRS develops a series of industrial software and hardware systems, enabled through biometric technology, which help Airports, Oil & Gas facilities and other “Critical Safe Secure” environments operate effectively. URL: www.hrsid.com
- Implant Sciences Corporation: IMSC designs, manufactures, and sells explosives trace detection and drugs trace detection solutions for aviation, transportation, customs, air cargo, critical infrastructure protection, ports and borders, force protection, public safety, and emergency responders. URL: http://www.implantsciences.com

- L-3 Communications: it is a supplier of security detection systems focussing on checkpoint, checked baggage and air cargo, at airports, transportation centers, ports and borders, secure government and commercial facilities, and events. URL: http://www.sds.l-3com.com
- Leidos Holdings: Leidos has more than 14,000 employees focused on key areas of national security, including intelligence surveillance and reconnaissance, integrated systems, mission support, and cybersecurity measures. URL: https://www.leidos.com/natsec/solutions
- Morpho Detection: It is a French multinational company developing explosives, narcotics and chemical detection systems used for many sectors such as transportation and critical infrastructure. URL: http://www.morpho.com
- NUCTECH: it is one of the main providers of security scanning equipment at global level. Their portfolio includes products for passenger baggage and perimeter security inspection. URL: http://www.nuctech.com
- Honeywell: Honeywell is a global expert in security and control technologies. URL: http://honeywell.com/Solutions-Technologies/Pages/security.aspx

### 3.2.4 Research and academic

The research and academic community will be interested in SECONOMICS results in a variety of ways. The following list summarises the main reasons for the interest of academic and research community in the project results:

- Preparation of course materials based on the project experiences and prepared textbooks (primarily universities).
- Introduction of some of the methods and tools available for public usage in lectures at universities in a form of practical usage (primarily universities, though also institutes through guest lectures).
- Application of the SECONOMICS outcomes in new research or to new scenarios.

# 4 SWOT ANALYSIS

This section addresses the exploitation of the whole SECONOMICS policy framework and toolkit and analyses the aspects contributing as well as hindering their further exploitation.

## Strengths

- SECONOMICS provides innovative integrated models to support stakeholders' decision making in security and economic matters. SECONOMICS framework and toolkit evaluate three main aspects: economic, technology, societal. The evaluation of the socioeconomic context is a major innovation with respect to existing approaches. The result is a unique and well balanced practice guidance.
- The models can be used in a nice and intuitive user interface. The tool integrating the models is also interoperable and portable. The various horizontal (across case studies) and vertical (across modelling strategies) approaches within SECONOMICS are supported by a broad set of software tools and appropriately specified infographics.
- SECONOMICS takes into consideration many security concerns from all stakeholders and agents involved and assessed thoroughly the strong and interactive relationships that exist between them. It is therefore a powerful tool to provide persuasive reasoning and communicate with involving stakeholders for a broad range of critical infrastructures.
- The comprehensive validation process in the project case studies ensures the reliability of the results.
- SECONOMICS comprehensively analyses very complex information such as the security decisions and preferences at many levels, i.e. supra-national, national, regional government and corporate levels.
- The explicit treatment of strategic antagonists generating security threats represents a further innovative aspect of SECONOMICS. This strategic element is accomplished by use of decision trees and extensive game theory analysis.

## Weaknesses

- The project has a strong research and prototype character, thus the results are not ready for immediate commercialization, and require further investment to reach the market.
- The ARA analysis and the associated models are very complex, making the task of customisation and re-use very complicated. In turn, the tool integrating the models requires a good knowledge of the underlying models for a proper use. As a result the customisation to new scenarios presents some challenges and a multidisciplinary team is needed, requiring sophisticated consultants.
- The Java interface also presents scalability and computational challenges.

- Research in the airport domain shows that additional cost variables should be considered, such as cost related to cancelation of flights, disruptions, loss of human lives, etc. As a starting point the values for cost-benefit analysis provided by EUROCONTROL may be used.

### Opportunities

- Research in the airport domain shows that policy decisions need to cover both IT and physical security, and include both direct and indirect cost, both for potential security incidents and for the investment in security measures. SECONOMICS policy tool therefore targets both security measure investment policy decisions and crisis management and disaster recovery policy decisions.
- Research on the UK National Grid case study showed that the main policy decision challenges are aligned with the objectives of SECONOMICS. These challenges include:
  - To assess and catalogue the interactions of security policy on the operation of critical national infrastructure (CNI) and the interaction with national and supra-national stakeholders/regulators and the wider European public.
  - How are various security concerns viewed from within a provider of CNI and from outside by its stakeholders.
  - To provide good practice guidance on how to implement security policy for CNI, balance cost and risk and communication of these trade-offs to the relevant stake holders.
- SECONOMICS also offers solutions that are aligned with the main security requirements that concern the urban transport authorities. Transport operators need to invest in security to increase the number of passengers and revenue.
- Urban transport systems share common characteristics as far as security is concerned. Such characteristics range from the high volume of passenger and the need for quick and easy access to the underground, local trains, buses or trams, to their operation along fixed routes with predetermined stops. This can facilitate the implementation of models and tools for new clients / transport systems such as buses and trams.
- In times of public budget constraints, SECONOMICS represents an opportunity to balance cost and security and ensure a balanced security resource allocation.

### Threats

- SECONOMIC modelling tools might lead to methodological changes for decision making. However, many organisations might have a reluctant attitude towards methodological changes.
- Limitations in the degree of operation discretion of critical infrastructure operators might impede the adoption of SECONOMICS results. In many cases, such as in the airport security domain, the degree of operational discretion is extremely limited. In the case of bulk-electricity transmission the operator has full discretion in security policy although decisions are taken in very close

cooperation with the relevant public bodies. The situation in the regional transport domain lies somewhere in between these two boundaries.

- Competition in the market segments is strong. It will be difficult to enter the market if one is not already well-positioned. Also, as has already been mentioned, some results require further developments, and could be marketed in 2016 or 2017. By then, these products and services might be less innovative.
- The outcomes of the validation reflected the experience that if the toolkit is used by consultants when being presented to policy makers, policy makers tend to be acutely interested in the technical detail and models behind the graphic interface of the toolkit. Therefore, the key academics involved would need to present that aspect of the toolkit so that the correct interpretation of the economic outcomes can be made.

# 5 Joint Business Strategy

## 5.1 Service portfolio

This section outlines an exploitation strategy with an emphasis on the commercial exploitation at consortium level, including guidelines to the deployment of the product/services the consortium wants to exploit.

The consortium or a partner can generate profit from the sale of different products and services, however two aspects constrain the potential commercial exploitation strategies: i) SECONOMICS results are publicly available without proprietary licences, and ii) it was not the aim of the project to develop off-the-shelf products, instead the consortium will enrich their consulting services exploiting modelling and customisations of existing components and results.

The SECONOMICS service portfolio includes the following lines of business:

- **Consulting services**:
  - **Advice on optimal security measures for operators**. The knowledge and findings gathered by the consortium with the numerous results (research and policy studies and use case toolkits) allow us to provide recommendations and advice on optimal security measures.
  - **Development of security models for policy makers.** This involves application, adaptation and calibration of models with parameters for new users and environments.
  - **Deployment services**. Whenever a client decides to deploy a decision support system based on the SECONOMICS Toolkit, the consortium can take care of the deployment of this technology without disrupting productivity of the user. This service involves adding new equipment and ensuring a smooth transition to operational phase.

- **Licensing of the toolkit or its parts.** The consortium has decided to make the SECONOMICS Toolkit available with an open source license in order to boost adoption of the SECONOMICS Good Practice by policy makers.[3] This is one of the cases where "putting foreground in the public domain constitute an appropriate alternative, taking into account the specificity of the project, the nature of the results concerned and the legitimate interests" of the public at large (see "Guide to Intellectual Property Rules for FP7 projects", p. 12). This is also justified by the current validation results which strongly suggest that a significant part of the 'Confidence Building' step is building the confidence in the expertise of the model designer, as opposed to the pure functioning of the software tool. However, as the consultancy services consolidate and prove successful over time, and a consensus over the policy models is built, the SECONOMICS Consortium or some of its partners might consider the option of developing a commercial

[3] GNU Lesser General Public License (LGPL v.3.0), see http://www.gnu.org/licenses/lgpl-3.0.en.html

product from the current open-source prototype in order to license the usage of this product for commercial uses. This product may also include new policy models built after the end of the project (pending agreement with their owners).

Two main billing models can be considered for the above service portfolio:

- **Support service fee**: fees for services such as consultancy, training, and further development services will be determined on the basis of man-days required on a project basis.
- **Subscription model**: Whenever possible the consortium will seek a recurring subscription billing, e.g. annual fee, for the cost of consultancy and other support tasks.

The role of the SECONOMICS partners can be classified according to their organization profile and lines of business, that is:

- **Research and academic partners** that may carry out new research activities built upon SECONOMICS results. This includes research institutes and universities. Partners under this category include UNITN, Fraunhofer, URJC, UNIABDN, AU, UDUR, ISASCR
- **Consulting companies**: partners that offer consulting services on regulation and security measures, as well as provide support regarding methodologies and technology used in the process, customer support and training. Partners under this category include DBL, Fraunhofer, NGRID, Atos and URJC.
- **Technology providers and system integrators**, which might develop new features for the toolset. They deliver complete systems based on the integration of different components. Partners under this category include Fraunhofer and Atos.
- **Infrastructure operator partners** will apply results to their own infrastructure (or collaborators) and produce recommendations to regulators. Partners under this category include NGRID, TMB.

One partner may perform more than one of the roles above.

## 5.2 Joint exploitation

The SECONOMICS consortium carried out an initial exercise to explore opportunities for joint exploitation. Bilateral talks have already started and the consortium is currently discussing collaboration agreements among partners to exploit SECONOMICS in the next years. Within this task the consortium identified the following categories of collaboration and related aspects to be considered:

1. **R&D projects**, which could be used to exploit SECONOMICS results. The SECONOMICS partners are interested in collaborating in further projects which represent an opportunity to exploit the project results. The following EU programmes (currently with open and forthcoming calls) offer potential for collaborations:
    - Mobility for Growth programme, e.g. MG-8.4a-2015: smart governance, network resilience and streamlined delivery of infrastructure innovation.

   - Fight against crime and terrorism programme, e.g. FCT-15-2015: ethical/societal dimension topic 3: better understanding the role of new social media networks and their use for public security purposes.
   - Digital security: cybersecurity, privacy and trust, e.g. DS-03-2015: the role of ICT in critical infrastructure protection.
   - Border security and external security programme.
2. Further development of results. As mentioned above many project results have a research and prototype character and require further development to be exploited beyond the research context. The consortium identified the following items as the more promising opportunities in this area:
   - To exploit the SECONOMICS Toolkit as a whole, expert support will be needed in order to implement the appropriate ARA models. Therefore, it is expected that future cooperation between the academic, technology providers and/or consulting companies will continue to effectively drive the project impact to the market. On the academic side URJC expects to contribute with risks analysts from their Statistics and Operational Research group. Fraunhofer, UDUR and DBL are also interested to explore this possibility.
   - DBL & ISASCR are discussing the possibility to team up to use the 'Coding technique for Salience Analysis in the Media' and the 'Media analysis of security perception by citizens' in consultancy services.
   - An extension of the considered decision making contexts. SECONOMICS models can be extended to different contexts if necessary. Contexts to be considered include: bus and tram infrastructures

## 5.3 IPR management and licensing

The outcomes that are jointly owned by multiple partners were covered by the existing project Consortium Agreement during the project lifetime.

In order to protect the outcomes after the project's end and choose appropriate license models the consortium conducted an exercise to identify IPR protection requirements. As a result of the survey, it was agreed that licensing the IPR was not necessary or applicable to any result (except for the SECONOMICS Toolkit which is licensed as open-source as explained above). It is therefore understood that each partner has the right to exploit the knowledge and any result outside the consortium.

The consortium partners are currently evaluating the suitability of an Exploitation Agreement which might cover IPR aspects in rather high level terms. Although this Exploitation Agreement is not necessary for IPR purposes it would represent a mechanism to encourage partners to look for synergies with other partners for the definition of new business opportunities, commercialization of the SECONOMICS results and other activity relevant for the benefit of the consortium. In any case, commercial exploitation of the IPR will be discussed whenever a specific commercial opportunity may arise.

# 6 Individual exploitation plans

This section describes the exploitation strategy at individual partner level

## 6.1 Universitá Degli Studi di Trento

As a high level academic institution, UNITN has performed the continuous exploitation of various project results. The experience and results obtained from projects has served as a basis for teaching materials in university courses and for new research. This makes UNITN have high scientific reputation at the national and international levels.
In this project, UNITN collaborates with other institutions, businesses and organizations to foster better outcomes and achievement, and will exploit the results in the following ways:

- The results will be used as inputs for other projects. In particular, UNITN will use results of the project to infuse them into several ongoing and starting projects.
- UNITN will exploit the results by using them as a basis for consulting, teaching and research activities. This will make UNITN advance the state-of-the-art in consulting, teaching and research.
- New ways to boost and facilitate collaborative research process between academia and industry will be developed. In addition, collaboration with the people in the current project will be sustained and further developed, even after the end of the project.
- Finally, UNITN will disseminate the research results via the standard academic and research channels: articles in the professional and technical press and scientific journals, communications and presentations at conferences, and professional exhibitions. These will promote technology and knowledge transfer.

## 6.2 Deep Blue

Deep Blue will mainly exploit SECONOMICS results in its consultancy and training activities for public and private organisations in the Airport and Air Traffic Management domains. The problem of integration of physical and logical security in complex environments such as Airports will become explosive in the future, because of the current predominant attention just on physical security, combined with the constant trend towards increased automation and communication, and the use of more open environments. SECONOMICS solutions will represent a very important contribution for the SESAR programme (targeted to the re-definition and management of Single European Sky in next decades). Ensuring new methods and tools to carry out an innovative Security Risk Assessment integrated with Socio-economical aspects will provide a significant commercial advantage to the companies that have developed and formalised the related concepts in the Civil Aviation Domain.
Societal and economical aspects, together with a proper communication of Security issues to passengers and airport operators will become very relevant for Policy makers, Regulators and Industries in the Aviation domain.

Secondly Deep Blue will further re-adapt SECONOMICS solutions and ideas in future R&D proposals and projects on similar topics, also exploiting SECONOMICS partnerships and collaborations.

## 6.3 Fraunhofer Gesellschaft zur Förderung der angewandten Forschung

Fraunhofer ISST and its third-party TU Dortmund have performed the continuous exploitation of various project results. The experience and results obtained from the project have served as a basis for teaching materials in university courses at TU Dortmund and for new research at both ISST and TUD. They contribute further to ISST's and TUD's high scientific reputation at the national and international levels. ISST will also exploit SECONOMICS results in its consultancy and training activities for public and private organisations in various domains, such as the Business Process Management and IT security. As ISST provides consultancy in security risk analysis, we will in particular exploit results on business modelling and risk analysis and management. We will also exploit the SECONOMICS framework and tool support.

In this project, ISST and TUD collaborate with other institutions, businesses and organizations to foster better outcomes and achievement, and will exploit the results in the following ways:

- ISST will present how results from SECONOMICS assist decision makers in national critical infrastructure during meetings with our industrial partners from the relevant domain.
- ISST will transform SECONOMICS results into our own knowledge and apply to the development of our risk assessment consultancy work.
- The results will be used as inputs for other projects. In particular, ISST and TUD will build on SECONOMICS solutions and ideas in future R&D proposals and projects on similar topics, also exploiting SECONOMICS partnerships and collaborations.
- ISST and TUD will exploit the results by using them as a basis for consulting and research activities. Furthermore, TUD will exploit the results by using them as a basis for teaching activities. This will contribute to enabling ISST and TUD to advance the state-of-the-art in consulting, teaching and research.
- New ways to boost and facilitate collaborative research process between academia and industry will be developed. In addition, collaboration with the people in the current project will be sustained and further developed, even after the end of the project.
- ISST and TUD will disseminate the research results via the standard academic and research channels: articles in the professional and technical press and scientific journals, communications and presentations at conferences, and professional exhibitions. These will promote technology and knowledge transfer.
- ISST will further contribute to SECONOMICS exploitation via industrial training through the provision of professional and corporate courses to potential users.
- ISST is currently in negotiation with industrial partners in order to jointly develop the open-source prototype of the SECONOMICS Toolkit developed in the project into a product to be licensed under a commercial license.

## 6.4 Universidad Rey Juan Carlos

The URJC team will exploit their SECONOMICS outcomes through:

- Improving their courses in related matters such as Decision Analysis, Risk Analysis, Game theory and, largely, Statistics and Operations Research.
- Publishing papers and monographs in the general area of security resource allocation.
- Reusing the knowledge generated in preparing further research proposals, possibly in cooperation with some of the current partners, not only in the area of CIP security, but also in other areas in which ARA may be applied (auctions, cybersecurity, computational marketing,…).
- Undertaking consulting opportunities in the broad area of security, as well as in other areas in which ARA may be applied.
- Developing MSc and PhD projects in relation with ARA.
- Integrating and interfacing ARA with traditional risk analysis methodologies.

## 6.5 The University Court of the University of Aberdeen

The University of Aberdeen has made a strong commitment to ongoing digital and physical security research in conjunction with other digital economy activities undertaken within the institution.

Exploitation is divided into two main areas although substantial overlap is desired and anticipated.

- Research: The stimulus provided by coordinating and working on the SECONOMICS project has and will be matched by ongoing investment in staff dedicated to security research. In particular the area of the economics of information security and the ongoing relationship with operational risk has featured a great deal of input from staff associated to the SECONOMICS project. We have currently, and intend to do so in the future, pursued both local and international funding opportunities in this area and have formed a ket research centre with fellow partner NGRID.
- Teaching: the work of SECONOMICS has impacted teaching in both the use of SECONOMICS case studies in taught programs in business and management and computing science. We envisage that a dedicated course with SECONOMICS outcomes will be included in our taught MSC programs in the next few years and in particular we hope to include this in management as well as technical programs.
- Finally, the direct exploitation for the university will be in the form of research outputs directly attributable to the project and the associated impact case studies used in the 2014 Research Excellence Framework, from which out major central government research funding is obtained. The case studies in SECONOMICS are the centre-piece to the business school in this area.

## 6.6 Ferrocarril Metropolita de Barcelona

TMB, as an urban public transport operator, which is fully committed with the quality of the product that produce and the satisfaction of our customer, works hardy to improve all the aspects that are critical in the service done. One of the main issues is the security of our passengers, who have to travel without any inconvenience during the experience of moving from place to another. In this line, TMB will use the results of the project to improve in an effective way the use of the different formulas, strategically, tactical and organizational that impact in the security in metro. The experience developed during the project is shared with other operators which can not only take advance but also suggests improvements in the solutions developed.

## 6.7 Atos Spain

Atos is a global IT services provider. SECONOMICS' "Recommendations on public policy for security" represents an opportunity to strengthen our portfolio on security consulting in the areas of compliance with international and national regulations, security risk assessment, gap analysis, awareness, and risk management and business intelligence integration.

The requirements collected for the urban train scenario and subsequent analysis developed during the project are an added value not only for Atos' public transport market but also for big events. Atos is an Information Technology Partner for the Olympic and Paralympics Games (2002-2024). Atos also provides cyber security advice, design build and operate services to its clients and has a strong alliance network (McAfee, RSA, Dell, NetIQ).

Atos will target the following possible channels to contribute to SECONOMICS exploitation:

- Joint programs between Atos Spain and other companies of Atos group. Within this program, Atos Spain will seek technology transfer to the product organization, and assist in the productization of those results, aiming to maximise effect at commercial level.
- Presentation of SECONOMICS technology in executive meetings, especially with subject matter experts in the Transport and Security domains.
- Industrial training through the provision of professional and corporate courses to potential users.

## 6.8 Secure Nok AS

As Secure-NOK AS specializes in security incident handling and security risk analysis, we are very interested in risk and business modelling results of WP5 and WP6. Results from those WPs will enrich our knowledge in risk analysis and management. We are also interested in the generalized version of the SECONOMICS framework and tools support for the framework developed in WP8. As we are developing our own risk assessment software, collaborating with other partners and gaining more experience and knowledge in these areas will help us in developing our risk assessment tool.

Through our industrial and academics networks, Secure-NOK will exploit SECONOMICS results in a number of ways:

- Integrate part of SECONOMICS results into an Information Security Economics course offered at a Norwegian university.
- Present how results from SECONOMICS assist decision makers in national critical infrastructure during meetings with our partners from an industrial consortium for Oil & Gas.
- Transform SECONOMICS results into our own knowledge and apply to the development of our risk assessment software.

## 6.9 Institute of Sociology of the Academy of Sciences of the Czech Republic

IS AS CR will utilize the results of SECONOMICS – in particular the new approaches combining social science, economics, mathematical perspectives on threats and risk, their perceptions and trade-offs – in its primary and applied research including the study of public opinion, as well as in consultancy for public bodies and civil society. The tensions and trade-offs between security, economics and privacy/freedom are becoming focal point of media, public and policy debates. In times, when understanding and acceptance of security measures varies culturally and cross-nationally, it is very important not only to address these topical questions academically, but also raise awareness within and beyond the academic community. IS AS CR therefore publishes its findings for broader audience in English in Prague SECONOMICS Discussion Papers, which are available in electronic form on the website of IS AS CR, for scientific community in form of papers and lectures at academic conferences and workshops. For policy makers in form of policy consultancy and policy briefs.

## 6.10 National Grid

National Grid, as a critical national infrastructure (CNI) provider is predominantly interested in the results of the Economics and Systems modelling work with SECONOMICS. In particular, National Grid is keen to seen how these models can be applied to incentivising a critical infrastructure provider to be secure against information and cyber security risks.

In the UK and Europe, CNI providers have lacked appropriate regulation around information and cyber security. Whilst some CNI providers have implemented robust and proactive risk management processes with dedicated security personnel, others have not sufficiently dealt with the security risks that their organisation is subject. Regulators in Europe have caught on to this and recently there has been the ‘threat’ of tougher regulation in this space.

With the Economic and System models, National Grid hopes to understand which methods best incentivise CNI providers to identify and mitigate against security risks. In turn National Grid, along with SECONOMICS project partners, will produce recommendations for the regulatory regimes that can be used as a vehicle to deliver the correct incentives.

National Grid aims to present these regulatory recommendations to regulators in the UK, Europe and other countries in which it operates, specifically the US. These regulators include the Department of Energy and Climate Change in the UK, the European Commission and its multiple Directorate Generals and the Department of Energy in the US. In addition, National Grid will present the outcomes of SECONOMICS to relevant agencies and industry groups who are key influencers to the regulators mentioned above. These include the Centre for Protection of National Infrastructure in the UK, Energy Networks Association in the UK and the European Network of Transmission Service Operators for Electricity amongst others.

## 6.11 Anadolu University, School of Civil Aviation

Anadolu University will take a role with the SECONOMICS experience and results mainly for training and consultancy in Civil Aviation and Air Traffic Management (ATM) domain. The ATM role in the aviation security is very important and effects flight operation's safety and capacity efficiency. ATM is becoming more central for future's aviation projects as SESAR and Nextgen. On the other hand, security operations related to ATM is not well known in the aviation environment. AU will take responsibility to disseminate of SECONOMICS outputs in Turkey and its region. SECONOMICS results will help to the high level stakeholders as Civil Aviation Authorities, Air Navigation Service Providers, Aviation-Airport Security Providers and decision makers. AU will exploit the results and experiences in the following ways:

- AU will exploit results for training, research, consulting and its airport operations. This experience will create added value for high and operational level of civil aviation for Turkey and its region.
- AU will disseminate results by academic papers in scientific journals, presentations, communications, discussions in conferences and workshops at national and international levels.
- The collaboration with the different and qualified international partners gives unique experience and opportunities for the future projects where AU could contribute related to civil aviation and ATM operations.

## 6.12 The University of Durham

The University of Durham will continue to support the ongoing work of Professor Williams' team after the completion of the SECONOMICS project and this support is reflected in the creation of an ongoing research cluster in the quantitative aspects of risk management folded into the finance and economics centre headed by the lead investigator on the project.

Exploitation is divided into two main areas although substantial overlap is desired and anticipated.

- Research: there is an ongoing research theme built around cooperation with the University of Trento and National Grid, research partners in the project.
- We have an ongoing multi-disciplinary research setting combining Computer Science and Economics in the Institute of Advanced Research in Computing and this is reflected in the association of the PIs with this major university research initiative.
- Teaching: the work of SECONOMICS will be expected to impact teaching in both the use of SECONOMICS case studies in taught programs in economics, business & management. We envisage that a dedicated course with SECONOMICS outcomes will be included in our taught MSC programs in the next few years and in particular we hope to include this in management as well as technical programs, this is likely to be included in the taught PG programme from January 2016.
- Finally, the direct exploitation for the university will be in the form of research outputs directly attributable to the project and the associated impact case studies used in the 2014 Research Excellence Framework, from which out major

central government research funding is obtained. The case studies in SECONOMICS are the centre-piece to the business school in this area.

## 7 Conclusions

SECONOMICS aimed at developing a policy toolkit that can effectively assist decision makers in identifying and reacting to public transportation and critical infrastructure threats. For this purpose SECONOMICS has used the latest technological tools available to develop state of the art security modelling, and has performed cutting edge risk assessments and analysis of the social context to support the development of optimal policies.

An assessment of exploitation activities conducted within the project reveals a number of opportunities for the uptake of the project results.

- The assessment of global trends and projections indicates growth potential for security solutions. Increased crime, accidents, antisocial behaviour, and continuous terrorist attacks have forced governments to spend a huge amount on transportation safety and security needs by providing high-tech integrated systems and services.
- There is evidence that solutions for technology-driven, automated and highly secure transportation and electricity transportation are needed. A common generic measurement tool (i.e. a cybersecurity capability maturity model that covers technology, regulatory, educational and operational dimensions) is needed.
- The feedback from the conducted research shows that training programmes for personnel responsible for security is needed. The EU authorities are already studying how to improve the recruitment and training of security guards. Current training and work modes are heterogeneous, causing gaps in protection.
- Each time a change is introduced new regulatory approach is required. Regulation needs to address many aspects such as mandatory cybersecurity standards, certifications and guidelines, technology, social and operational dimensions.

In this context with so many security measures available and different aspects to be considered within the transportation and critical infrastructure and security domains, the best practices and tools developed within SECONOMICS can be of great benefit for all stakeholders involved.

# 8 References

Topnews.in, ‘New Zealand says full airport security too expensive’, May 2009, available from: http://topnews.in/new-zealand-says-full-airport-security-too-expensive-2167867. [Accessed 13 January 2015]

Frost and Sullivan, ‘An Overview Of The Airport Security Market’, November 2009, available from: http://www.slideshare.net/tony.ridley/an-overview-of-the-airport-security-market. [Accessed 13 January 2015]

BCC Research LLC, ‘Global Transportation Security Market To Reach $5.9 Billion In 2016’, September 2011. Available from: http://www.bccresearch.com/pressroom/ias/global-transportation-security-market-reach-$5.9-billion-2016. [Accessed 13 January 2015]

Transport Canada, ‘Outlook, Trends and Future Issues’, 2012. Available from: https://www.tc.gc.ca/eng/policy/anre-menu-3024.htm. [Accessed 13 January 2015]

Marketsandmarkets.com, ‘Transportation Safety and Transportation Security Market [Modes (Airways; Seaways; Roadways; Railways); Systems (Access Control; Surveillance, Scanning, Screening, Tracking, Navigation, Fire Safety)] - Global Forecasts and Analysis (2013 – 2018)’, November 2013, available from http://www.marketsandmarkets.com/Market-Reports/transportation-safety-security-market-1287.html?gclid=CMSa_ujd_MICFWjItAoda1AAHg

PRNewswire, ‘Transportation Safety and Transportation Security Market Modes (Airways; Seaways; Roadways; Railways); Systems (Access Control; Surveillance, Scanning, Screening, Tracking, Navigation, Fire Safety): - Worldwide Market Forecasts (2013 - 2018)’, December 2013. Available from: http://www.prnewswire.com/news-releases/transportation-safety-and-transportation-security-market-modes-airways-seaways-roadways-railways-systems-access-control-surveillance-scanning-screening-tracking-navigation-fire-safety---worldwide-market-forecasts--235600211.html. [Accessed 13 January 2015]

TENACE project, “Critical Infrastructure Protection: Threats, Attacks and Countermeasures”, March 2014, available from http://www.dis.uniroma1.it/~tenace/download/deliverable/Report_tenace.pdf

Frost and Sullivan, ‘Global Airport Security Market Assessment Update Security Upgrade Needs Show Pressure Points in Airport Security Expenditures’, April 2014, available from: http://www.marketresearch.com/product/sample-8140676.pdf. [Accessed 13 January 2015]

Visiongain, ‘Aviation Security Market Forecast 2014-2024 Prospects for Leading Companies in Cargo, Passenger, Airline & Airport Security’, July 2014. Available from: https://www.visiongain.com/Report/1296/Aviation-Security-Market-Forecast-2014-2024. [Accessed 13 January 2015] von Hirschhausen C., Holz F., Gerbaulet C., Lorenz C., ‘European Energy Sector: Large Investments Required for Sustainability and Supply Security’, July 2014, available from: http://www.diw.de/documents/publikationen/73/diw_01.c.469268.de/diw_econ_bull_2014-07-6.pdf

UITP, ‘October 2014 Statistics brief world metro figures’, available from: http://www.uitp.org/sites/default/files/cck-focus-papers-files/Metro%20report%20Stat%20brief-web_oct2014.pdf

SECUR-ED project, ‘White paper for public transport stakeholders’, November 2014, available from: http://www.secur-ed.eu/wp-content/uploads/2014/12/SECUR-ED_White_Paper_Final.pdf.

UK Regulators Network, OFGEM, ‘UK Regulated Infrastructure, An Investor Guide’, December 2014, available from: https://www.ofgem.gov.uk/ofgem-publications/91882/ukrninvestorguide.pdf

World pop, ‘EU prepares more controls to strengthen aviation security’, January 2015, available from: http://worldpop.org/eu-prepares-more-controls-to-strengthen-aviation-security/. [Accessed 13 January 2015]