SECONOMICS

D9.8 - First Stakeholders' panel report

Iván Zaldívar (Atos), Alessandra Tedeschi (DBL), Raminder Ruprai (NGRID), Michael Pellot (TMB)

Pending of approval from the Research Executive Agency - EC

Document Number	D9.8
Document Title	First Stakeholders' panel report
Version	1.0
Status	Final
Work Package	WP 9
Deliverable Type	Report
Contractual Date of Delivery	31.01.2014
Actual Date of Delivery	10.04.2014
Responsible Unit	ATOS
Contributors	UNITN, DBL, NGRID, TMB, SNOK
Keyword List	Stakeholders' panel, community, airport, CNI, Urban public transport
Dissemination level	PU

SECONOMICS Consortium

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

1	UNIVERSITÀ DEGLI STUDI DI TRENTO	Università Degli Studi di Trento (UNITN) 38100 Trento, Italy www.unitn.it	Project Manager: prof. Fabio Massacci Fabio.Massacci@unitn.it
2	DEEPBLUE	DEEP BLUE Srl (DBL) 00193 Roma, Italy www.dblue.it	Contact: Alessandra Tedeschi Alessandra.tedeschi@dblue.it
3	Fraunhofer ISST	Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., Hansastr. 27c, 80686 Munich, Germany http://www.fraunhofer.de/	Contact: Prof. Jan Jürjens jan.juerjens@isst.fraunhofer.de
4	Universidad Rey Juan Carlos	UNIVERSIDAD REY JUAN CARLOS, Calle TulipanS/N, 28933, Mostoles (Madrid), Spain	Contact: Prof. David Rios Insua david.rios@urjc.es
5	UNIVERSITY OF ABERDEEN	THE UNIVERSITY COURT OF THE UNIVERSITY OF ABERDEEN, a Scottish charity (No. SC013683) whose principal administrative office is at King's College Regent Walk, AB24 3FX, Aberdeen, United Kingdom http://www.abdn.ac.uk/	Contact: Prof. Matthew Collinson matthew.collinson@abdn.ac.uk
6	TMB Transports Metropolitans de Barcelona	FERROCARRIL METROPOLITA DE BARCELONA SA, Carrer 60 Zona Franca, 21-23, 08040, Barcelona, Spain http://www.tmb.cat/ca/home	Contact: Michael Pellot mpellot@tmb.cat
7	Atos	ATOS SPAIN SOCIEDAD ANONIMA ESPANOLA, Calle Albarracin, 25, 28037, Madrid, Spain http://es.atos.net/es-es/	Contact: Alicia García Medina alicia.garcia@atos.net
8	SECURENOK	SECURE-NOK AS, Professor Olav Hanssensvei, 7A, 4021, Stavanger , Norway Postadress: P.O. Box 8034, 4068, Stavanger, Norway http://www.securenok.com/	Contact: Siv Houmb sivhoumb@securenok.com
9	SOÚ Institute of Sociology AS CR	INSTITUTE OF SOCIOLOGY OF THE ACADEMY OF SCIENCES OF THE CZECH REPUBLIC PUBLIC RESEARCH INSTITUTION, Jilska 1, 11000, Praha 1, Czech Republic http://www.soc.cas.cz/	Contact: Dr Zdenka Mansfeldová zdenka.mansfeldova@soc.cas.cz
10	nationalgrid THE POWER OF ACTION	NATIONAL GRID ELECTRICITY TRANSMISSION PLC, The Strand, 1-3, WC2N 5EH, London, United Kingdom	Contact: Dr. Raminder Ruprai Raminder.Ruprai@uk.ngrid.com
11	ANADOLU ÜNİVERSİTESİ	ANADOLU UNIVERSITY, SCHOOL OF CIVIL AVIATION Iki Eylul Kampusu, 26470, Eskisehir, Turkey	Contact: Nalan Ergun nergun@anadolu.edu.tr
12	Durham University	The Palatine Centre, Stockton Road, Durham, DH1 3LE, UK	Contact: Prof. Julian Williams julian.williams@durham.ac.uk

Document change record

Version	Date	Status	Author (Unit)	Description
0.1	25/06/2013	Draft	Iván Zaldívar (ATOS)	Table of Content definition
0.2	05/11/2013	Draft	Iván Zaldívar (ATOS)	Changes in the document structure
0.3	19/02/2014	Draft	Alessandra Tedeschi (DBL)	Airport Case Study Section added.
0.3	04/03/2014	Draft	Michael Pellot (TMB)	Urban public transport Case Study Section added.
0.4	05/03/2014	Draft	Iván Zaldívar (ATOS)	Final Draft version with contributions from WP1 and WP3 collated
0.5	10/03/2014	Draft	Woohyun Shim, Elisa Chiarani (UNITN)	Quality check completed. Some changes and comments to be addressed
0.6	13/03/2014	Draft	Iván Zaldívar	Reviews from Quality check addressed
0.7	21/03/2014	Draft	Raminder Ruprai	Final draft version with contribution from WP2
0.8	27/03/2014	Draft	Iván Zaldívar	Changes requested during the review in the General Assembly and from the first technical review.
0.9	07/04/2014	Draft	Woohyun Shim, Elisa Chiarani (UNITN)	Second quality check completed. Some changes and comments to be addressed
0.10	08/04/2014	Draft	Aitor Couce Vieira, Steve Randall (SNOK)	Scientific Review. Comments provided
1.0	10/04/2014	Final	Iván Zaldívar	Changes after technical review (SNOK) and quality check (UNITN)

INDEX

Executive summary

This report presents the first results of the community building task within WP9 of the SECONOMICS project. The information has been gathered from each of the case studies of the project as defined in the D9.2 [1].

In sections 2, 3 and 4, the detailed information about stakeholders, events, status and impact of the panel is presented for each case study. Specifically, the impact from each of the panels can be summarised as follows:

- The Airport case study Stakeholder Panel consists of National and European institutions in the Aviation domain, Civil Aviation Authorities and Air Navigation Service Providers. Preliminary feedback and discussion were generally positive and promising, with some concerns with respect to possibly high costs of implementing the SECONOMICS tools and guidelines, their complete compliance with existing regulations at European level and the effort needed in the modelling phase, since great expertise is required.
- The CNI case study Stakeholder Panel consists of the internal NGRID Security leadership, a UK Government Agency and the European group of Electricity Transmission System Operators. The feedback following the CNI validation activities has been positive and promising and the next steps are to focus the validation activities on the national and supranational panel members.
- The urban public transport case study Stakeholder Panel consists of city security leadership, public transport operators' security entities and international urban public transport operator's security leadership. The feedback following the public transport case study validation and discussion activities has been very fruitful and promising and the next steps are to focus the validation activities on the national and international panel members.

In general, the feedback collected from the panels have been very useful, serving initially as a starting point for gathering the case studies requirements and scenarios and ultimately (at the current stage of the project) for the model validation process.

The information gathered has also helped in identifying the areas perceived by the stakeholders to be less useful, allowing for refinement of the work done and providing a focus on these aspects to improve the final result.

Additionally, section 5 of this document presents a new category of stakeholders that is being investigated, expanding the community into a new area which has been identified as potentially interesting for the whole project.

Finally, it can be concluded that the work done in the panels has identified the current strengths of the project and is serving to draw the general lines in which the solution should be based to constitute a cost-effective tool able to help the policy makers in creating common rules across the European Union.

1. Introduction

The first stakeholders' panel report gathers and presents the results of the three case studies as part of the community building task within the SECONOMICS project.

The change in the name of the report (from users' panel report to stakeholders' panel report) is due to a light change in the task itself: Rather than organising specific events to engage the stakeholders, it has been identified by the consortium that using the different events and workshops within each case study for both disseminating the project and collecting feedback, will be a more practical and productive way to create a community that serves the purpose of the project.

The three case studies cover:

- WP1: Airport Security
- WP2: Critical Power Infrastructure
- WP3: Regional and Urban Transport

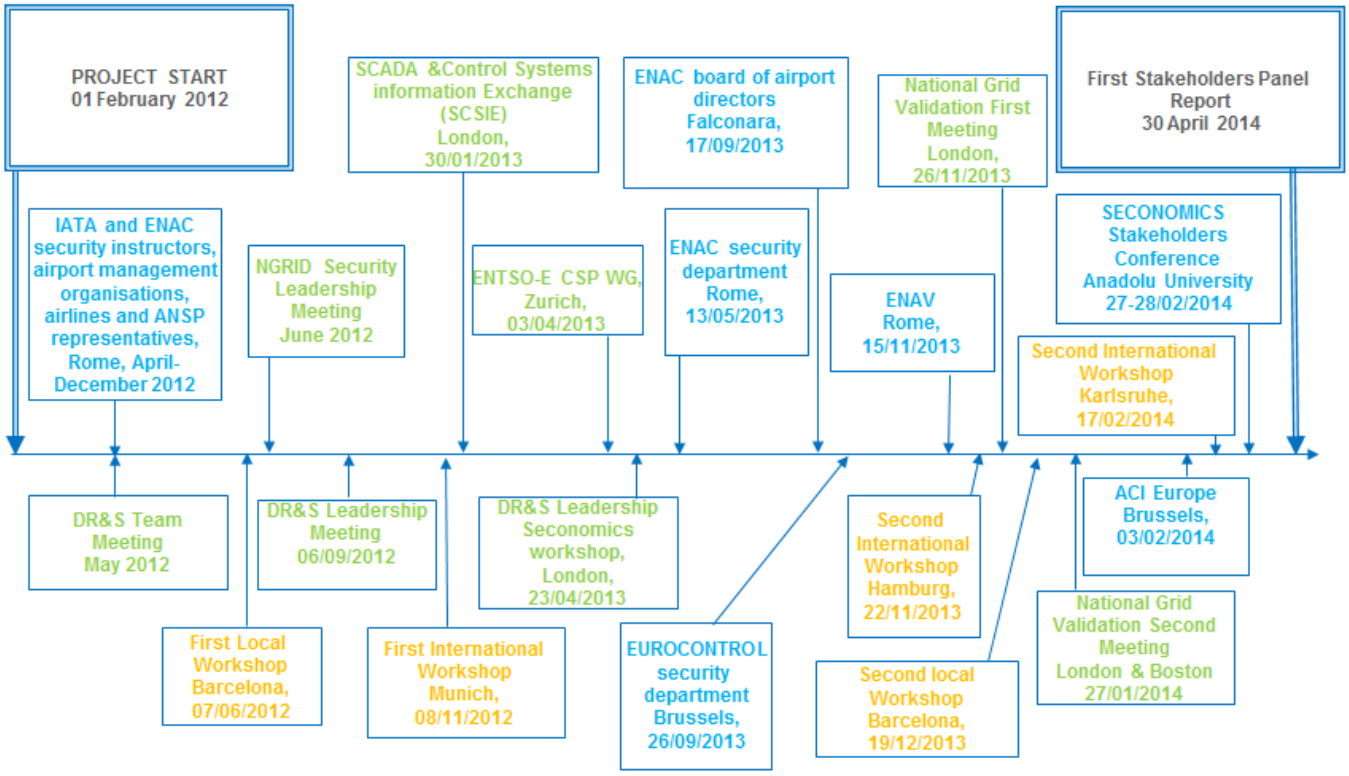

Figure 1 Panels' Events Timeline

As can be seen in figure 1, several events have been held for each panel during this period, with several of them working towards Pan-European Coordination by involving stakeholders from various European countries.

The methodologies for the panels were defined in D9.2 and were followed by the SECONOMICS partners with minimal changes in order to achieve the objective in the most efficient manner. During this period of the project, monthly meetings were held and the persons responsible for the community building activities had a chance to report

and review the progress of the tasks and plans, the next steps and events in close relation with the dissemination activities so that both were able to work for the benefit of the project.

As an update to the information presented in the previous community building deliverable, D9.2, the coordinator of the CNI panel activities will be (and has been during the work on this specific panel) the NGRID representative, Raminder Ruprai.

The next sections of the document show the information for each of the panels in an agreed structure, add a possible new stakeholders' category and finish with common conclusions extracted from the work done in each of the panels.

2. Airport stakeholders' panel

2.1 Stakeholders

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

2.2 Events

Event	Purpose	Participants
Iterative Meetings with IATA and ENAC Security Instructors, Airport Management Organisations, Airlines and ANSPs representatives, Rome, April-December 2012	Define Airport Security requirements and WP1 scenarios	2 Deep Blue people, 2 ENAC certified Security Instructors, Rome Airport Security Managers, ENAV Security Manager, Alitalia and Meridiana former Security Managers.
ENAC Security Department Meeting, Rome, 13/05/2013	Present SECONOMICS Project scope and approaches	2 Deep Blue people, 2 ENAC Representatives.

Event	Purpose	Participants
ENAC Board of Airport Directors Meeting, Falconara, 17/09/2013	Present and discuss SECONOMICS Project scope and approaches.	3 Deep Blue people, 2 people UNITN, 15 ENAC Board of Airport Directors.
EUROCONTROL Security Department Meeting, Brussels, 26/09/2013	Present and discuss SECONOMICS Project and collect feedback and comments from decision makers at European level.	2 Deep Blue people, 3 Eurocontrol Security Department officers.
ENAV Meeting, Rome, 15/11/2013	Present and discuss SECONOMICS Project and collect feedback and comments from an ANSP perspective.	3 Deep Blue people, 1 UNITN people, 4 ENAV Safety Department officers, 3 ENAV Security Department officers.
ACI Europe, Brussels, 03/02/2014	Present and discuss SECONOMICS Project and collect feedback and comments from an airport management perspective.	1 person from Deep Blue, 2 ACI Europe Security Department officers.
SECONOMICS Stakeholder Conference, Anadolu University - Eskisehir, 27-28/02/2014	Present and discuss SECONOMICS Project with European Aviation Stakeholders.	6 SECONOMICS Consortium Members, about 25 SECONOMICS stakeholders, speakers and participants.

2.3 Panel information

2.3.1 Stakeholders' panel in detail

During this period of the project, DeepBlue has worked with ENAC (national), ACI Europe, Eurocontrol and ENAV. More details about these stakeholders and their involvement in the project are presented below:

- **ENAC** is the Italian Civil Aviation Authority, the "Ente Nazionale per l'Aviazione Civile". Their mission is to propose and approve national aviation legislations compliant with international standards and to enforce regulatory compliance by different civil aviation stakeholders.
- **ACI - Europe** represents the interests of over 450 airports in 44 European countries. ACI members account for over 90% of commercial air traffic in Europe. ACI membership is comprised of airport operators of all sizes, along with national airport associations, world business partners and educational establishments working together in an active association to ensure effective communication and advocacy with legislative, commercial, technical, environmental, passenger and other interests.
- **Eurocontrol**, the European Organisation for the Safety of Air Navigation, is an international organisation founded in 1960 and composed of Member States from the European region, including the European community which became a member

in 2002. Their main missions are (a) to support its Member States in achieving safe, efficient and environmentally-friendly air traffic operations across the European region; and (b) to deliver the "Single European Sky" of the 21st century. To achieve its objectives, the Eurocontrol Agency works closely with Member States, air navigation service providers (ANSPs), civil and military airspace users, airports, the aerospace industry, professional organisations, intergovernmental organisations and the European institutions.

- **ENAV S.p.A.** is the company which provides the Air Traffic Control service and other essential services for air navigation, in the Italian Skies and in the national airports, with a consistently improved level of safety, efficiency and punctuality.

2.3.2 Current state and near future of the Aviation Security

Aviation security is a strongly regulated domain. Regulations, mandatory procedures and internal rules to ensure Security standards compliance must be respected.

In the SECONOMICS project, identifying and studying the nature and state of policies and regulations forms a key objective of the analysis. Deep Blue and Anadolu University carried out a state of the art review of current European and worldwide regulations and discussed relevant threats and vulnerabilities with Airport security stakeholders to select proper scenarios for the Airport Case Study.

Many of the threats, generic vulnerabilities and exploitations in current and future scenarios have been identified and described in D1.3 [2].

In detail, the International Civil Aviation Organization (ICAO) [3] specifies minimum standards which every State must satisfy in order to be a member (and, thus, to be permitted to have flights originating, terminating and transiting its own territory). This means that every Member State is required to build a civil aviation structure, which must satisfy the minimum standards and share it with the rest of the world. Members States can create a different organisation, as European Union Members did, creating ECAC (European Civil Aviation Conference). Each Member State is required to draw up a National civil aviation Security Programme (NSP).

An NSP defines the general rules for each airport operator, airline etc. which should be followed in terms of airport and on-board security, passengers, luggage, mail and goods screening, airport and on-board supply, recruitment and training for personnel.

Airports will become more and more complex and tightly coupled systems with many interacting stakeholders with different roles and responsibilities as well as opposing interests.

Ensuring security, compliance with regulations and law, business and economic interests and the preservation of passengers rights and needs will be a significant challenge for policy and decision makers (both at European and a local level).

Moreover, new security threats, such as sophisticated cyber-attacks or bio-attacks will arise.

2.3.3 Impact of the stakeholders' panel events

As stated above, aviation security is a strongly regulated domain. Convincing policy makers and regulators, both at national and European levels, of the effectiveness and

usefulness of the SECONOMICS approach should be a significant goal. To assure this objective, DBL in cooperation with other project partners has organized five main activities with high-level Aviation Security policy makers at national and European levels.

During the first 9 months of the projects regular meetings with Airport Security stakeholders have been carried out in order to elicit Airport Security Requirements and Scenarios.

On 13th May 2013, DBL presented the SECONOMICS project objectives and preliminary results to two members of the Security and Safety Departments of ENAC.

On 17th September 2013 DBL and UNITN presented SECONOMICS to the "Board of Airport Directors". The Board encompasses the ENAC Directors of the major Italian Airports and it holds bimonthly meetings by discussing policy and regulatory proposals to be presented and approved by competent Authorities.

On 26th of September 2013 DBL presented SECONOMICS, together with other Security-related projects, to three members of the Eurocontrol Security Department.

On November 15th 2013 DBL presented, together with UNITN, the SECONOMICS project and models to ENAV Security and Safety Department representatives.

On February 3rd 2013 DBL joined ACI Europe Security Managers in Brussels to present the SECONOMICS models and results for the Airport Case Study in detail.

Finally, on February 27th and 28th 2014 the SECONOMICS Stakeholder Conference has been held in Anadolu University, Turkey.

The Airport Case Study partners' main aim was to collect preliminary feedback and comments from the stakeholders regarding the applicability and suitability of the SECONOMICS results in the Airport Domain.

All the involved stakeholders were really interested in the SECONOMICS project and their preliminary feedback about the project scope and methodologies was positive. An approach encompassing security, economics and societal aspects in an integrated way that analyses and balances risk, costs and passenger acceptance of airport security measures has been considered as promising and very useful for decision and policy makers in the aviation domain.

According to Eurocontrol and ENAC representative members, SECONOMICS will ease system modelling and analysis, communication and information sharing with different airport stakeholders (ranging from managers, politicians and regulators to front-end operators and passengers associations) and will effectively support decision making for policy makers and airport security managers. Also WP4's media analysis results were considered really interesting and useful.

ENAV and ACI Europe were particularly interested in the modelling and analysis of the Cyber-threat Scenario that is an emerging open issue in the domain.

ACI Europe was also positively impressed by the WP6 modelling activity which was considered to be very promising for the support of the on-going discussion on 'customised policies and incentives' among the Airport Community and the European Regulators.

Some multi-faceted feedback was gathered: on one hand, the Airport Security domain could accept SECONOMICS solutions because of the potential and innovation of the approach to the provision of a Decision Supporting Tools and guidelines that integrate Risk Assessment, advanced Cost Benefit Analysis and Social aspects. On the other hand, it might be difficult for the Airport Security domain to accept SECONOMICS because of existing regulation, standard processes and work-practices widely adopted.

In order to foster its adoption, the SECONOMICS solution should be cost-effective and easy to use. A possible exploitation model should include support for the modelling and quantitative analysis part as an additional consultancy service.

2.3.4 Panel conclusions

Preliminary feedback and discussion were generally positive and promising, although there were some concerns with regard to the possibly high costs of SECONOMICS tools and guidelines, their compliance with existing European regulations level and the effort and skills needed in the modelling phase (significant expertise is required). The SECONOMICS consortium has started to incorporate this feedback in the scenarios and models and customize its solutions for the Airport and Aviation domain proposing viable business models.

3. CNI stakeholders' panel

3.1 Stakeholders

Stakeholder panel member/organization	Relevant information
Digital Risk & Security (DR&S)	Internal National Grid information and cyber security team for its operations globally (UK and US). Provides security governance, strategy, architecture, policy, operations and consultancy across the entire organisation including Electricity Transmission in the UK.
UK Government Agencies and Regulators	This set of organisations includes: 1.) Department of Energy and Climate Change (DECC) is the government department which is charged with the responsibility to manage all aspects of energy and climate change in the UK. National Grid has a very important relationship with DECC as this is the government department it reports to with regards to its regulated duties. 2.) Centre for the Protection of National Infrastructure (CPNI) is a UK government agency, which is part of the intelligence services, whose duty it is to ensure that all aspects of critical national infrastructure in the UK are protected.
European Network of Transmission System Operators for Electricity (ENTSO-E) - Cyber Security Group	ENTSO-E is a group which brings together all the electricity transmission operators across Europe, National Grid included. It provides a forum for the transmission operators to discuss ideas, progress and changes in different areas of the industry. There is a specific Cyber Security working group

	of ENTSO-E where cyber security issues are presented and discussed, which National Grid chairs.

3.2 Events

Event	Purpose	Participants
DR&S Team Meeting, Teleconference,May 2012	Introduce Seconomics and the aims and outcomes of WP2	DR&S Global Team (Approx 35 people)
NGRID Security Leadership Meeting, Teleconference, June 2012	Introduce Seconomics and the aims and outcomes of WP2	NGRID CIO, NGRID CISO, NGRID Head of Physical Security (Approx 10 people)
DR&S Leadership Meeting Teleconference, 06-09-2012	Electricity Transmission Threats Brainstorm	DR&S Leadership team including NGRID CISO (8 people)
SCADA & Control Systems Information Exchange (SCSIE), London, 30-01-2013	Introduce Seconomics, present the year 1 work of WP2 and the overall aims and objectives of WP2. Discuss the possible uses by the members of SCSIE and UK Regulators.	CPNI, Other UK CNI operators (Approx 30 people)
ENTSO-E CSP WG, Zurich, 03-04-2013	Introduce Seconomics, present the year 1 work of WP2 and the overall aims and objectives of WP2. Discuss the possible uses by European Regulators and other TSOs	European Transmission System Operators (TSOs) (Approx 15 people)
DR&S Leadership Seconomics Workshop, London, 23-04-2013	Discussion of the Economics and System models proposed by UNIABDN and data required to calibrate the models	DR&S Leadership team including NGRID CISO, UNIABDN (11 people)
National Grid Validation First Meeting, London, 26-11-2013	Detailed discussion of the current state of the WP2 models with a focus on how the models would meet the aims of the case study	DR&S Leadership team including NGRID CISO, UNIABDN (10 people)
National Grid Validation Second Meeting, London & Boston videoconference, 27-01-2014	Detailed discussion of the updated WP2 models with a focus on key questions to calibrate the models specifically to the real-life setting of a CNI operator	DR&S Leadership team including NGRID CISO, UNIABDN (10 people)

3.3 Panel information

3.3.1 Stakeholders' panel in detail

National Grid's main stakeholder groups are DR&S (internally within National Grid), CPNI (national) and ENTSO-E (supranational) as described in the table above. More details of these stakeholder groups are given below including their interest and involvement in SECONOMICS.

- **DR&S** in the UK is tasked with managing and mitigating the cyber security risks within National Grid UK through security strategy, governance, risk, compliance, consulting, architecture, and threat and incident management. WP2 has maintained a constant engagement with DR&S to understand current and future security threats and risks to National Grid's business and the current regulatory requirements. In addition, the Chief Information Security Officer (CISO) of National Grid is the main sponsor of the company's involvement in the SECONOMICS project.
- **CPNI** is a UK government agency, which is part of the intelligence services, whose duty is to ensure that all aspects of critical national infrastructure in the UK are protected. This includes, but is not limited, to availability, physical security, information security and the protection of reputation. As National Grid owns and operates CNI, CPNI provides guidance and advice on many of these aspects of security. CPNI also provides guidance directly to government departments including DECC. Therefore we plan to engage further with CPNI on their views of different regulatory frameworks and share with them the output of the SECONOMICS project so that this can be fed back to the energy regulators nationally.
- **ENTSO-E** is the group of European electricity transmission service operators (TSO). Their CSP working group is made up of cyber security experts from each TSO who discuss and put together papers that can enter standards and law governing network operations across Europe. National Grid is represented in this group by the DR&S Head of Operational and Information Technology. This is the main stakeholder group of the CNI case study at a European level and will provide a forum for surveying different regulatory structures across the TSOs, present working models from WP4, 5 and 6 and discuss policy papers.

3.3.2 Current state and near future of the Critical National Infrastructure

CNI providers are an example of organisations whose risks have potential impacts beyond the organisation on citizens and society. Governments have a responsibility of ensuring that those organisations identify, understand and appropriately mitigate the security risks.

National Grid, as the electricity transmitter in the UK, is a CNI provider and there are numerous risks to electricity transmission that affect everyone connected to it. Many of the threats, generic vulnerabilities and exploitations both in the current and future states have been described in Deliverable D2.3 [4]. In particular, the future and emerging threats and risks to CNI were broken down into different views which looked at the impact, opportunity, threat actors & motives and means. National Grid's overall opinion was that the future landscape of energy delivery was changing with the

development and implementation of smart grids and SCADA systems becoming more complex and connected to the internet. As a result the threat landscape would increase in future. To add to this, the fast pace of IT innovation will provide future attackers with continually increasing means of attacking CNI. Consequently, an increasing range of threat actors with higher capabilities and motivation to attack CNI can be expected in the future.

The key concern of governmental regulators is how best to ensure such information risks and cyber security risks to CNI and their operators are appropriately mitigated. Another way of looking at this problem is as follows: How can the CNI operators be incentivised to identify and mitigate the security risks that have the potential to impact the CNI and beyond? Governments have been solving and continue to solve this problem using regulation and this is one of the key aims of WP2.

3.3.3 Impact of the stakeholders' panel events

As National Grid's information and cyber security function, DR&S are keen to understand how different regulatory structures would incentivise the business best in order to be secure. Whilst there is a well-established, rules-based regulatory scheme in the USA, no such scheme exists in the UK or Europe. DR&S would like to drive the debate in this area with the regulators so that the best regulatory scheme for all parties is implemented.

To this end a number of events have taken place with different members of DR&S to present and discuss different areas of the SECONOMICS project. The high level aims and objectives of WP2 have been presented to the entire DR&S global team in both years 1 and 2 of the project. In addition, a number of calibration and validation workshops were organised with members of the DR&S leadership including the National Grid CISO to discuss and agree the modelling approaches being taken and the data that would be required by UNIABDN/UDUR to calibrate the proposed models they are building in WP2 for the CNI case study.

An initial model review and data gathering workshop was held in April 2013 between the DR&S leadership which was very useful for applying the generic models presented in WP6 to the CNI case study setting.

Following numerous workshops between NGRID and UNIABDN the models were refined and then presented back to the DR&S leadership in two validation meetings. The aims and purpose of each model were presented in detail and very specific refinement questions were discussed around each model which will help to produce more realistic and accurate models. Whilst the model building, calibration and refinement has been and continues to be an iterative process, significant progress has been made towards applying the models to the specific CNI case study for the purpose of analytically comparing the different regulatory systems.

At a European level, National Grid is keen to drive the debate around regulation of CNI industries so that any regulatory structure that is implemented in the future is optimal for all parties. ENTSO-E Cyber Security Group is the best candidate for discussing the models at a European level. The members of ENTSO-E, as TSOs for all the European countries, will be able to validate the models against the operation of their CNI and provide feedback. Following this, the ENTSO-E Cyber Security Group provides the perfect platform for presenting the outcomes from these models which they can then present back to their respective national regulators.

In April 2013 the SECONOMICS project and WP2 in particular was presented to the ENTSO-E Cyber Security Group. Once the models have been refined, the next steps will be to present the models and their various outcomes to the other members of the CNI Stakeholder Panel namely the CPNI nationally and ENTSO-E CSP at the European level.

3.3.4 Panel conclusions

Summarising, feedback and discussions with the DR&S leadership has been positive and promising. There were some pointed questions from the group about how the models would produce useful outcomes. These were clarified by UNIABDN and UDUR to the satisfaction of the DR&S leadership.

Initial feedback from the CPNI, following a presentation on SECONOMICS and WP2 at the SCSIE meeting in January 2013, was very positive and they are looking forward to seeing the refined models when they are ready.

The ENTSO-E CSP group are keen to see models that produce actionable information or recommendations that they can discuss with their national regulators and feed up into the European regulators. This feedback has been fed to UNIABDN and UDUR as the models are being refined and the outcomes of the models are being determined.

4. Urban public transport stakeholders' panel

4.1 Stakeholders

Stakeholder panel member/organization	Relevant information
UITP - International Association of Public Transport	UITP is organized by Commissions and Committees. The Security Commission (SecComm) studies, assesses and promotes innovative operation and technology for enhanced Public Transport Security
Mossos d'Escuadra - Regional police	Official Police Force in the region of Catalonia. It has an organised group specialized in Public Transport and Rail services.
Spanish Urban transport operators	Different spanish urban railway operators performing similar services as TMB does in Barcelona.

4.2 Events

Event	Purpose	Participants
First local Workshop, Barcelona, 07/6/2012	Present SECONOMICS Project scope and approach. Development of possible Scenarios.	TMB, ATOS, Mossos d'Escuadra. (including 1 police commander and 3 TMB's security managers)
First International Workshop, Munich, 08/11/2012	Present SECONOMICS Project scope and approach. Validation and Feedback of possible Scenarios.	TMB, UITP SecComm (including 16 operators, 3 international public transport associations and 1 security association).
Second International Workshop, Hamburg,	Present and discuss final approach of scenarios,	TMB, UITP SecComm (including 18 operators, 3 international public transport associations and 1

Event	Purpose	Participants
22/11/2013	development and feedback of the societal approach.	representative of the European Commission).
Second local Workshop, Barcelona, 19/12/2013	Present and discuss final approach of scenarios, development and feedback of the societal approach. Development and feedback of the Risk Analysis Models.	TMB, ATOS, Mossos d'Escuadra, Metro Bilbao Security manager, IS ASCR, URJC. (including 3 police commanders, 1 National Metro operator security manager and 2 TMB's security managers)
Second International Workshop, Karlsruhe, 17/2/2014	Present the final model for the societal approach and feedback of the Risk Analysis Models.	TMB, UITP SecComm (including 16 operators, 2 international public transport associations and 1 security association).

4.3 Panel information

4.3.1 Stakeholders' panel in detail

TMB's main stakeholders are UITP (international), Spanish urban transport operators (national) and Mossos d'Escuadra (regional) covering all ranges and giving specific feedback from different levels. More details about these stakeholders are presented below:

- **UITP** is the International Association of Public Transport. It is a non-profit international association and internationally recognized because of its work to advance the development of a critical policy agenda. UITP has a long history to its name, and is the only worldwide network bringing together all public transport stakeholders and all sustainable transport modes.

  The UITP governance structure is composed by bodies, mainly Commissions and Committees. One of those Commissions is the Security Commission (SecCom).

- **Mossos d'Escuadra.** Regional police of Catalonia. The Mossos d'Esquadra is an integral police force with a defined model, functions and structure. The Catalan model is based on the development of the Police Force of Catalonia, comprising the Police Force of the Generalitat and the local police force. Cooperation, collaboration, institutional fidelity and mutual assistance between the authorities, administrative bodies and public services are the main principles of the Catalan system of public safety. It is a police force at the service of the community, closely linked to the needs of the society it serves. Its main values are its commitment, its professionalism and its proximity to the people it serves.

- **Spanish Urban transport operators**. A group of Spanish public transport operators that have similar missions and tasks as TMB in Barcelona and, therefore, similar problems and ways to solve them. Included in this group are local operators from the same area where TMB operates. They can provide input for requirements and validation of models and tools as they deal with similar issues on a day to day basis. Operators are being involved throughout the project lifecycle with dissemination activities and in the provision of feedback.

4.3.2 Current state and near future of Urban public transport

TMB is the main urban transport operator in the Barcelona Metropolitan area and, with 730 million passengers per year, deals daily with multiple security incidents involving passengers, security staff and facilities. Security in the subway is closely integrated with the security model of the city. Thus, the laws and procedures applied in cases of incidents which affect the subway are the same ones applied to other incidents in the city, but the conditions in a closed space make the risks severer than in an open place. Many of the threats, generic vulnerabilities and exploitations both in the current and future states have been described in Deliverable D3.3 [5]. In particular, the urban transport scenarios based on existing and emerging threats were described and the key validation indicators were provided.

From the stakeholders' point of view, even though the security incidents have not changed too much, the background has evolved significantly. For example, transnational organizations (e.g. organized fare evasion) are orchestrating criminal activities. In addition, the use of new information technologies and the proliferation of anti-social behaviour require a new approach to overcome these new security scenarios.

The security forces (Mossos d'esquadra, National Police, Civil Guard and local Police of the affected municipalities), courts, fire-fighters and emergency services, neighbourhood associations and councils are directly involved, and the public transport operators work hard to raise awareness and facilitate the actions needed.

Besides the models identified initially in the transport case study, graffiti and vandalism are also a clear concern as they are becoming not only a regional or national problem but a transnational problem. Transport operators are affected by internationally organized crime networks traveling around Europe to "express their art". Graffiti is a growing trend in the transport sector that creates operational, financial and reputation losses and it needs to be addressed.

Another example of an emerging threat affecting railway transport in general and urban transport in particular is metal theft. Metal thieves target signaling cables, overhead power lines and even metal fences to be sold as scrap. When a cable is cut, and because of the way railway networks are designed, the trains are stopped and the service is disrupted until the problem is fixed. The criminal networks behind these thefts are transnational, and the stolen metal is usually transported across several borders and sold as scrap away from the crime scene.

Although the framework is different in each country or even in each city, it is clear that the stakeholders and their responsibilities are similar. That is why it is so important to share information and get feedback from them. Even when the laws are different, the ways to tackle the different problems in each network are very similar.

4.3.3 Impact of the stakeholders' panel events

The main objective of the five workshops organized to date was to share the methodologies, the scope, the potential scenarios and the motivation of the project. After the first two workshops, which can be considered as part of the first phase of the project and aimed at identifying possible security scenarios, the focus of the remaining workshops was to discuss and rationalise the social and risk analysis models.

These workshops allowed validation and reinforcement, within each of the different phases, of all the concepts and models developed in the past two years of research.

In detail, the main goal of the first Workshop with stakeholders, held in June 2012, was to identify which scenarios have most impact on them. These scenarios were described in D3.2. The definition of those scenarios evolved with the contributions received mainly from transport stakeholders, and the final scenarios used in the definition of the models are those described in project report D3.3.

In the process of describing the scenarios, it was identified that is necessary to analyse and identify the motivations and causes that make the offenders participate in malicious activities, order to determine the appropriate measures to counteract the different types of incidents listed on each scenario. For example, an attacker's reasons for individual fraud are distinct from those for collective fraud; therefore the way to fight each type of fraud is different.

Three types of motivations were identified, initially drafted in project report D3.2, and later developed in project report D3.3: Uncivic behaviour, Antisocial behaviour and Criminal behaviour.

Scenarios and motivations identified in the project were presented to the expert group of the UITP Security Commission. The definitions of the scenarios as well as the motivations that were described in D3.3 were discussed within the UITP Security Commission, developing them to their current definitions included also in D3.3.

A survey was submitted to the UITP security commission members (formed by the security staff from urban transport operators) to gather, among other things, information on the security priorities in their organizations. The conclusion is that, in general, security issues related to passengers' real and perceived security and to facilities security are identified by the experts as the highest priorities.

Another conclusion worth mentioning relates to the answers to "which are the main social impacts taken into account for the decision making process related to the security dimension within the organizations". Most answers highlighted the internal acceptability and the internal policies of the organizations, legal aspects, public security and social and economic dimensions.

These answers suggest that, scenarios with an economic and social impact in the organizations (such as fraud) and scenarios with legal, security and social impact (such as pickpocketing) are the most popular among the transport operators.

Given the interests of the stakeholders and the existing and emerging threats reported in D3.3 document, the scenarios have been chosen accordingly. Additionally, in urban transport, social and risk dimensions potentially have a more severe impact given that urban transport is a mass transportation infrastructure and consequently, any security incident may have severe repercussions.

The main causes of emerging threats are the trans-nationality of the activities, the increasing activity by organized groups, both of an antisocial and a criminal nature, the introduction of new technologies having an impact in new security measures affecting the users and the use of these technologies by the organized groups mentioned above.

It can be summarized that the scenarios with the highest social and risk impact are fraud and Pickpocketing. Fraud also has a high economic impact.

The validation method and criteria are composed of two types of activities: validation activities and activities oriented towards promoting the model to similar organizations.

The specific validation activities with external experts are based on validation workshops, explaining the goals and the expected outcomes of the model, and a survey to check the usefulness of the model to the stakeholders considering the risks that the model tries to minimize. Feedback is collected for the models presented.

Two activities were initially planned for the evaluation with stakeholders. The first during the yearly meeting of the UITP Commission on Security (16th meeting in Hamburg) and a second which was a workshop with Urban transport related stakeholders. A third activity was scheduled later during the 17th meeting of the UITP Security Commission that was organized as an event at the IT-TRANS International Conference and Exhibition at Karlsruhe.

A 90 minutes slot was booked during the third activity for the presentation of the models from the SECONOMICS project. A summary of the following topics was presented and the feedback was collected through the questionnaires:

- Update of SECONOMICS project progress (goals and current state)
- Urban transport scenarios, analysis and selection
- Validation of security and society models
- Validation of risk analysis models

4.3.4 Panel conclusions

The feedback gathered and the discussions held were very positive in general terms. Although the law that regulates different cities and countries is different, this experience showed that the way to tackle security challenges by different operators is quite similar. This implies that while there are some local peculiarities in each city and those should be taken into account by the model, the SECONOMICS models and tools might be applicable to all of them.

As is mentioned in D3.4, in discussions with the Spanish police about the terrorism, it was clear they were interested on this particular problem (proof of that is that they request video recordings from TMB when necessary) but their specific reasons for investigating or raise a request are never disclosed to TMB security department. The police never disclosed their interest in terrorist activities as they are treated like any other security issue.

5. Possible additional stakeholders

Considering the work done in the study WPs and, therefore, the information extracted by industrial partners, it has been determined that the project could benefit from having an additional category of stakeholder in close relation with the scope of the project.

Although a cyber-terrorism threat is less likely right now, considering their main systems are not connected to the Internet, it can still be considered as a common and important

threat for all the case studies. Experts state that there are almost always semi-direct connections through routers shared between the control system and business systems that can be exploited and of course the specific case of Stuxnet is self-explanatory. Consequently, seems logical to search additional stakeholders with expertise in this particular area.

The consortium agreed to initiate efforts to find contacts connected to this area, with ENISA [6] and cyber security forums being the first two names brought to the discussion.

In this aspect, several events have been identified so that the project can "extend" its scope (referring to stakeholders) obtaining additional information, feedback and of course, disseminate the project.

The task is still in an initial state, but two events were considered for this purpose and strong efforts were made to find a niche in any or both events:

- Annual Privacy Forum 2014 (http://privacyforum.eu/).
- CSP Forum 2014 (https://www.cspforum.eu/2014/).

Finally, it is confirmed that a member of DBL will attend and speak in the CSP Forum 2014.

The task will evolve during the remaining lifecycle of the project and the results will be presented in the second stakeholders' panel report in M36.

6. Conclusions

The results of the panels so far can be considered promising and very positive. The project goals have been presented in several meetings, workshops and conferences and were well received by all the stakeholders involved. During these events, the information received has been very useful both for gathering information on the initial requirements and scenarios and for validating the models developed in the project.

Furthermore, this feedback has helped in detecting the main areas perceived as problematic, making it possible to focus efforts on developing a strong and useful solution.

The summarized information can be seen in this SWOT [7] matrix:

Strengths	**Weakness**
- Project goals well received. - Positive feedback from the work done so far. - Good expectations of the results of the project.	- Complete compliance with the current European regulations hard to achieve. - Differences in regulations between countries or regions.
Opportunities - Solution able to cover new and emerging problems. - Creation of unified rules along the	**Threats** - Not managing to develop a cost effective solution. - Usability (only usable by end users

European Union.	with great expertise).

Therefore, it can be concluded that the project must focus on developing a cost-effective solution that should be attractive to end users with different levels of expertise. On the other hand, the project has the potential to create a product able to cover current problematic as well as new emerging threats, ultimately helping European policy-makers to create common regulation within the European territory.

The next steps in the community building task, in addition to continuing with the same activities for the remaining time of the project, are organizing a final project event that will present the results of the whole project. This event will try to involve the main stakeholders from each panel.

REFERENCES

[1] D9.2 Users' panel definition and strategy - Silvia Castellvi (2012).
[2] D1.3 Airport Requirements final version – A. Tedeschi (2013).
[3] International Civil Aviation Organization (http://www.icao.int/Pages/default.aspx).
[4] D2.3 National Grid Requirements final version – Raminder Ruprai (2013).
[5] D3.3 Urban Public Transport Requirements final version – R. Munné, M. Pellot (2013).
[6] European Union Agency for Network and Information Security (http://www.enisa.europa.eu/).
[7] SWOT: Structured planning method to evaluate the **s**trengths, **w**eakness, **o**pportunities and **t**hreats in a project or business.