

SECONOMICS

D9.13 - Second Stakeholders' panel report


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

Pending of approval from the Research Executive Agency - EC

Document Number	D9.13
Document Title	Second Stakeholders' panel report
Version	1.2
Status	Final
Work Package	WP 9
Deliverable Type	Report
Contractual Date of Delivery	31.01.2015
Actual Date of Delivery	27.01.2015
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	 SOU Institute of Sociology AS CR	INSTITUTE OF SOCIOLOGY OF THE ACADEMY OF SCIENCES OF THE CZECH REPUBLIC PUBLIC RESEARCH INSTITUTION, Jilská 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 İki Eylül Kampusu, 26470, Eskisehir, Turkey	Contact: Nalan Ergun nergun@anadolu.edu.tr
12	 Durham University	The Palatine Centre, Stockton Road, Durham, DH1 3LE, UK	Contact: Prof. Julian Williams julian.williams@durham.ac.uk

Document change record

Version	Date	Status	Author (Unit)	Description
0.1	10/11/2014	Draft	Iván Zaldívar (ATOS)	Table of Content definition
0.2	05/12/2014	Draft	Iván Zaldívar (ATOS)	First draft of the document
0.3	19/12/2014	Draft	Iván Zaldívar (ATOS)	Second draft with contributions from SNOK (oil&gas) and DBL, NGRID, TMB (stakeholders and events)
0.4	09/01/2015	Draft	Iván Zaldívar (ATOS), Alessandra Tedeschi (DBL), Raminder Ruprai (NGRID), Michael Pellet (TMB)	Contributions from DBL, NGRID and TMB (impact and conclusion sections) for each panel
0.5	15/01/2015	Draft	Iván Zaldívar (ATOS), Aitor Couce (SNOK)	Changes after technical review from SNOK
0.6	21/01/2015	Draft	Elisa Chiarani (UNITN)	Quality check
1.0	26/01/2015	Draft	Iván Zaldívar (ATOS)	Final version after quality check
1.1	26/01/2015	Draft	Fabio Massacci (UNITN)	Final Review
1.2	27/01/2015	Final	Iván Zaldívar (ATOS)	Final version integrating comments from the project coordination

INDEX

Executive summary	5
1. Introduction	6
2. Stakeholders’ panel events	7
3. Airport stakeholders’ panel	10
3.1 Stakeholders’ panel in detail	10
3.2 Current state and near future of the Aviation Security.....	11
3.3 Impact of the stakeholders’ panel events	12
3.4 Panel conclusions.....	12
4. CNI stakeholders’ panel	13
4.1 Stakeholders’ panel in detail	13
4.2 Current state and near future of the Critical National Infrastructure.....	13
4.3 Impact of the stakeholders’ panel events	14
4.4 Panel conclusions.....	14
5. Urban public transport stakeholders’ panel	15
5.1 Stakeholders’ panel in detail	15
5.2 Current state and near future of Urban public transport.....	15
5.3 Impact of the stakeholders’ panel events	16
5.4 Panel conclusions.....	17
6. Stakeholders beyond SECONOMICS	17
7. SECONOMICS Summit.....	18
8. Conclusions	18
REFERENCES.....	20

Executive summary

This report presents the final 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 project deliverable D9.2 [1].

In a similar way than the previous stakeholders' report (D9.8), sections 2, 3, 4 and 5 present and update the detailed information about stakeholders, events, status and impact of the panel for each case study. For ease of reference, this deliverable summarizes the results of the stakeholders' engagement that SECONOMICS has achieved in the case study domains. Additional details can be found in the deliverables of WP1, WP2 and WP3.

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. The SECONOMICS toolkit has been appreciated and accepted by the stakeholders and they stated their intention to use and adopt the toolkit in their decisional process within the Airport Security domain.
- The Critical National Infrastructure (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. It was agreed by those stakeholders that the underlying models of the SECONOMICS toolkit inherently integrate the security, economic and social perspectives of CNI.
- 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 stakeholders were satisfied with the SECONOMICS toolkit and its approach to calculate the best resource allocation for a specific situation.

Section 6 of this document presents possible stakeholders beyond SECONOMICS, in this case, the specific sector detailed is oil&gas.

Section 7 provides with an overview of the final project event, the SECONOMICS Summit held in Brussels on the 5th of November.

Finally, it can be concluded that the work done in the panels has been essential during all the stages of the project and has helped developing the final results which have been positively evaluated by all the involved stakeholders.

1. Introduction

The second 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, as it was defined in the previous report) is due to a light change in the task itself: The consortium identified that, rather than organising specific events to engage the stakeholders, the use of different events and workshops within each case was a more practical and productive way to disseminate the project, collect feedback and create a community around the project.

The three case studies cover:

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

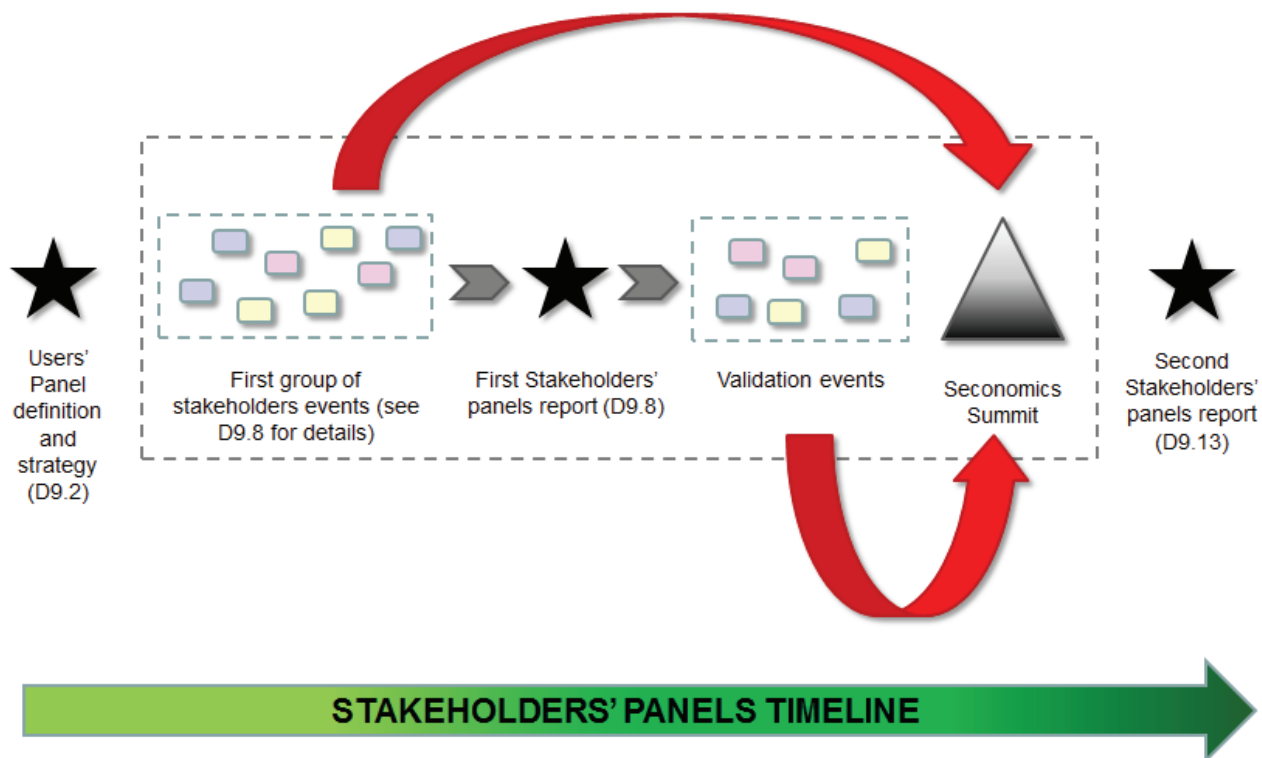


Figure 1 Stakeholders Panels' Timeline

As can be seen in figure 1, the strategy and methodologies for the panels were defined in the D9.2. During the first period of the project, several events were held for each panel working towards Pan-European Coordination by involving stakeholders from various countries. The results from this period were reported in the D9.8 [2].

During the last period of the project the activities with these stakeholders continued in the same direction, this time focused in validating the work done in the project and adjusting it into a final product with feasible exploitation results.

An important stakeholders' panel event (not only for the panels but for the whole project) was held in Brussels on the 5th of November: the SECONOMICS Summit. The Summit gathered different stakeholders from each panel plus additional ones to present current and future challenges, to show how the work done in the project interacts with/resolves these problems and exchange opinions about these topics between the stakeholders themselves and between the stakeholders and the SECONOMICS consortium.

The next sections of the document show the information for each of the panels in an agreed structure, add a possible new stakeholders' sector (oil&gas), summarizes the SECONOMICS Summit event results and finish with common conclusions extracted from the work done in each of the panels.

2. Stakeholders' panel events

The following table groups the events held during this period in each panel. Additional details about these events can be found in deliverables D1.5, D2.5 and D3.5:

Panel	Event	Purpose	Participants
Airport	Iterative Meetings (in presence or through conference calls) with IATA and ENAC Security Instructors, Airport Management Organisations, and Airlines representatives, Rome, April-December 2014.	Seconomics Model and Toolkit Validation.	2 Deep Blue people, 2 ENAC and IATA certified Security Instructors, Alitalia and Meridiana former Security Managers, Brno, Esbjerg, Ancona - Falconara, Pescara, Perugia, Rimini and Forlì Security Managers.
Airport	Conference Call with IATA Security Training Manager, September 2014.	Presentation of the SECONOMICS project and discussion about SECONOMICS main results.	1 DBL and 1 IATA representative.
Airport	Conference Call with Assoaeroporti Security Dept. Manager, September 2014.	Presentation of the SECONOMICS project and discussion about SECONOMICS main results.	1 DBL and 1 Assoaeroporti representative.
Airport	SECONOMICS Final Summit, Airport Case Study Validation Workshop, Brussels 5 November 2014.	Validation of the SECONOMICS toolkit.	2 DBL people, 2 UNITN people, 1 ISASCR people, 1 URJC people. 2 European Commission representatives (DG Airport Security and DG Move 2), 1 IATA representative, 1 CSP Forum representative.
Airport	SECONOMICS Final Summit, Aviation Security Panel, Brussels 5 November 2014.	Present and discuss SECONOMICS Project with European Aviation Stakeholders.	SECONOMICS Consortium Members, about 50 European stakeholders, speakers and participants.
CNI	CPNI Meeting, London, 7th May	Third validation meeting with the CPNI. CNI	NGRID, 2 CPNI representatives

Panel	Event	Purpose	Participants
	2014	Security Advisors from CPNI who cover the energy and utilities space. Focusing on the background and context of the CNI case study as well as both economic models at a high level.	
CNI	NGRID validation Meeting, London, 29th May 2014	Validation Meeting with the DR&S Leadership focused on calibrating the parameters of the Subsidy & Incentives (Agility) model part of the toolkit.	NGRID, UNIABD
CNI	ENTSO-E Cyber Group Meeting, Vienna, 3rd June 2014	Having introduced SECONOMICS and the CNI case study at a previous meeting, the meeting was focused on introducing and explaining in more detail the Subsidy & Incentives (Agility) model and the Policy Coordination (Sustainability & Resilience) model.	NGRID, ENTSO-E
CNI	UK Cabinet Office Meeting, London, 15th July 2014	The Cabinet Office advisors on the National Cyber Security Programme for the lead government departments had a keen interest in understanding the effects of different types of regulation on the security within CNI organisations. Presentation and the discussion focused on the background and context of the CNI case study as well as the Policy Coordination (Sustainability & Resilience) and Subsidy & Incentives (Agility) models at a high level.	NGRID, 3 UK Cabinet Office representatives
CNI	DECC Meeting, London, 22nd July 2014	Presentation and the discussion focused on the background and context of the CNI case study as well as the the Policy Coordination (Sustainability &	NGRID, UNIABD, 3 DECC representatives

Panel	Event	Purpose	Participants
		Resilience) and Subsidy & Incentives (Agility) models at a high level.	
CNI	NGRID validation meeting, London, 11th August 2014	Complete the calibration of the Policy Coordination (Sustainability & Resilience) model part of the toolkit, which is described here, and to present some initial outcomes of the toolkit.	NGRID, UDUR
CNI	ENTSO-E Cyber Group Meeting, Brussels, 18th September 2014	Building on the stakeholder buy-in built up in previous meetings, this meeting focused on calibration. Specifically the Policy Coordination (Sustainability & Resilience) model and gaining further insight and agreement on the calibration areas discussed in the NGRID Validation Meeting of the 18th of November	NGRID, ENTSO-E
CNI	SECONOMICS Final Summit, Critical infrastructures Panel, Brussels, 5th November 2014.	Present and discuss SECONOMICS Project with European Stakeholders.	SECONOMICS Consortium Members, about 50 European stakeholders, speakers and participants.
CNI	NGRID validation meeting, London, 10th November 2014	Presentation of several use cases and scenarios of the Subsidy & Incentives (Agility) model.	NGRID, UNIABD
CNI	ENTSO-E CSP Meeting, Cologne, 2nd December 2014	Build on the stakeholder buy-in built up in previous ENTSO-E Cyber group meetings to discuss where the work with SECONOMICS had reached and some initial outcomes, particularly around the Subsidy & Incentives (Agility) model.	NGRID, ENTSO-E
CNI	ENTSO-E CSP Meeting, Cologne, 3rd December 2014	Building on the stakeholder buy-in built up in previous meetings, this meeting focused on presenting scenarios built up from the Policy Coordination (Sustainability &	NGRID, ENTSO-E

Panel	Event	Purpose	Participants
		Resilience) model and detailed usecases/scenarios related to the phase diagram of the Subsidy & Incentives (Agility) model.	
Transport	First Validation workshop, Brussels , 4th November 2014	Validation of the Seconomics toolkit based on Urban transport models for Risk Analysis Models.	TMB, ATOS, ISAS CR, URJC, Mossos d'Escuadra (including 1 police commander)
Transport	SECONOMICS Final Summit, Public Transport Security Panel, Brussels, 5th November 2014.	Present and discuss SECONOMICS Project with European Stakeholders.	SECONOMICS Consortium Members, about 50 European stakeholders, speakers and participants.
Transport	Second validation Workshop, Barcelona, 9th December 2014	Validation of the Seconomics toolkit based on Urban transport models for Risk Analysis Models.	TMB, ATOS, Metro Bilbao Security manager, URJC. (including 1 National Metro operator security manager and 4 TMB's security managers)
Transport	Fourth International Workshop, Brussels, (Tentative date: 21st April 2015)	Present and discuss final results of the project in the form of project toolkit, feedback collected by TMB.	TMB, UITP SecComm. This is a forecasted event after the end of the project as to provide the final results to the UITP SecComm as one of the main stakeholders participating in the project. This was not possible to do before the end of the project due to the planning of UITP SecComm meetings.

3. Airport stakeholders' panel

3.1 Stakeholders' panel in detail

DeepBlue's main stakeholders are 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.
- **IATA**, the International Air Transport Association 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.
- **Assaeroporti** is the Trade Association of the Italian Airport Management Organisations. Assaeroporti includes 35 Airport Management Companies representing 39 Airports for a total value of 144 million passengers and 1.5 million flights.

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 is 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 [3].

In detail, the International Civil Aviation Organization (ICAO) [4] specifies minimum standards which every country 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 with the creation of the European Civil Aviation Conference (ECAC). 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.

Moreover, new security threats, such as sophisticated cyber-attacks or bio-attacks will arise. Therefore, ensuring security, compliance with regulations and law, business and economic interests and the preservation of passengers rights and needs will become an even more significant challenge for policy and decision makers (both at European and a local level).

3.3 Impact of the stakeholders' panel events

During this period of the project, several iterative meetings were held with the airport stakeholders. E-mail exchanges and conference calls complemented this engagement in a continuous and coherent manner.

IATA and ENAC Security Instructors, domain experts, Airport Management Organisations (such as AERDORICA and SAGA), Airlines representatives and International organizations were contacted regularly in order to involve and keep them updated about the project's research results, on both technical and theoretical concepts.

All this work was focused in presenting the overall framework of the project, its objectives and approach as well as the features of the airport security case study and the modelling approaches from WP5 and WP6. The stakeholders really appreciated the implementation of these models into the software tool and how they become real instruments for decision makers. They also provided recommendations to help developing the tool further.

After iterative refinements, validation sessions were maintained using group discussions, questionnaires, interviews, and audio visual recordings. The results from these sessions concluded that the toolkit was positively evaluated by the stakeholders.

3.4 Panel conclusions

The SECONOMICS toolkit has been appreciated and accepted by the stakeholders involved in the various panel sessions during the last year of the SECONOMICS project. They were satisfied with its functionalities and considered it as an efficient instrument for policy-makers in their decisional process.

The toolkit was evaluated as suitable for the Airport Security domain since it recognizably covers all the needed information and concepts required by such domain. By means of the involvement of a wide variety of professionals and experts, the knowledge represented in the toolkit has been made consistent and valid.

Even though not immediately ready-to-use, the stakeholders' panel members stated their intention to use and adopt the toolkit in their own decisional process within the Airport Security domain.

In summary, a general acceptance and appreciation of the mechanisms and computational strategies under the models has been achieved, due to the quality and

usefulness of the results and to the effective and user-friendly implementation of the tool.

4. CNI stakeholders' panel

4.1 Stakeholders' panel in detail

National Grid's main stakeholder groups are DR&S (internally within National Grid), CPNI (national) and ENTSO-E (supranational). 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.

4.2 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 D2.3 [5]. In particular, the future and emerging threats and risks to CNI were broken down into different views which looked at the impact, opportunities, threat actors, their motives and their means. National Grid's overall opinion is that the landscape of energy delivery is 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 the 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 to ensure that such information 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.

4.3 Impact of the stakeholders' panel events

The stakeholder panel members, DR&S Leadership, CPNI and ENTSO-E Cyber group, were engaged during this period of the project during several meetings and workshops. They were extremely interested in the scientific background of the economic models and how they could be used specifically in the CNI domain.

The policies presented in the validation meetings, as part of the complete policy landscape presented, were considered applicable and relevant to the CNI industry. In addition, the terminology remains consistent to that used within the CNI domain.

The stakeholders gave valuable and robust feedback over the validation sessions that led to iterative changes being implemented appropriately in the underlying models and overall tool.

Ultimately, their final feedback revealed a variety of beneficial results and outcomes. It was further agreed that these could be easily turned into policy and regulatory recommendations to meet the aims of the CNI case study and SECONOMICS.

4.4 Panel conclusions

The stakeholder panel members agreed that the models implemented inherently integrate the security, economic and social perspectives of CNI. The high complexity of the concepts exposed was positively estimated and the quality of the technical academic rigour demonstrated by the models was praised.

However, it was identified and agreed that interaction with experts simplifies the communication of key concepts, and the general impression was that the academic and industry experts behind the models should be present to facilitate and provide interpretation.

The interface was evaluated positively and the stakeholders' feedback indicates that the chosen approach visually presents the results in a clear, concise and useful manner.

5. Urban public transport stakeholders' panel

5.1 Stakeholders' panel in detail

TMB's main stakeholders are UITP (international), Spanish urban transport operators (national) and Mossos d'Esquadra (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'Esquadra.** 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.

5.2 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 D3.3 [6]. 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, Guardia Civil 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.

5.3 Impact of the stakeholders' panel events

The stakeholders in the urban public transport were engaged using two different approaches:

- Local stakeholders of TMB, other transport operators in Spain and the regional police.
- The International Association of Public Transport (UITP) as the main organisation grouping stakeholders in the Public Transport domain in Europe and worldwide.

Both groups of stakeholders have been continuously involved in the project activities, helping to shape the requirements and scenarios for the urban transport use case, during both the security and society and risk models validation, and finally on the toolkit validation, which implemented the risk models for the fare evasion and pickpockets' scenarios.

The stakeholders' engagement was mainly achieved on the validation workshops held with the local stakeholders and during the regular meetings of the UITP Security Commission. During the last year of the project, the toolkit validation sessions have been structured with a common approach in order to present the progress and gather feedback: presentation of the Security Risk Models approach, Toolkit Demo and live exercise with the toolkit with Security Risk Models (What-if), collection of feedback and suggestions through a structured survey.

5.4 Panel conclusions

The SECONOMICS toolkit has been positively evaluated by the stakeholders' panel members but they stated some considerations about specific aspects of the theoretical models implementation within the tool during the sessions held on the third year. The panel participants were satisfied with the approach of how the best resource allocation for a specific situation was calculated, however, the scenario at network level and the dynamics of a network transport (behaviour changes depending on the time, mobility of attackers along the transport network) were identified as interesting parts to be included.

Other than these considerations, they agreed that the security risk models can be extended to other types of threats where attackers and defenders want to maximise their effectiveness.

6. Stakeholders beyond SECONOMICS

SECONOMICS have had the participation of several stakeholders in the three case studies, demonstrating the interest and involvement with the project. Extending SECONOMICS to other critical infrastructure sectors would need to replicate the successful multi-perspective collaboration, and therefore a continuation of the systematic engagement of different kind of stakeholders.

In a potential Oil and Gas application, SECONOMICS should try to engage stakeholders of very different kinds to achieve a multi-perspective overview of the potential security scenarios to be addressed. The different groups of stakeholders that might participate in an Oil and Gas extension of the toolkit could be:

- Regulators on security and safety issues in Oil and Gas: This kind of organizations is the link between the high-level policies and regulations from the government or other security agencies and the sector players. They are the stakeholders that, by recommendation or enforcement, specify the security requirements and practices that have to be met. E.g., Bureau of Safety and Environmental Enforcement (USA), Petroleumstilsynet (Norway).
- Sector associations: This kind of organizations usually lead initiatives on the development of security recommendations or practices tailored to specific subsectors or installations. In addition, they represent the best forum to exchange feedback on the potential challenges and trade-offs of implementing a specific security policy at the operational and business level. E.g., Society of Petroleum Engineers, American Petroleum Institute.
- Other interesting types of stakeholders that might be considered to complete a stakeholders' panel are research centres in O&G (e.g., International Research Institute of Stavanger (Norway)).
- Companies (e.g., oil majors, drilling operators, and equipment and service suppliers).
- Representatives of the local, regional and national authorities of the areas with a high presence of O&G installations (e.g., North Sea or the Gulf of Mexico)

7. SECONOMICS Summit

On the 5th of November of 2014, the SECONOMICS Summit was held in Brussels (details about the venue, agenda, photos, etc. can be found in the D9.14 [7]).

Counting around 45-50 people from different organizations, the event started with a presentation of the project directed towards the whole audience. Afterwards, the airport security panellist presented and discussed several points such as how do socio-economic issues affect aviation security policies, challenges and opportunities in air traffic management security increasing automation and cyber-security, security training or how airport security could benefit from policies or standards and best practises from other domains.

The CNI panellists offered a real example of a Critical National Infrastructure and its security issues: the existence and assessment of different regulation approaches (depending on the country), topics like cyber-security and critical assets protection, and a presentation of the oil&gas sector and its security treatment.

The urban transport panellist covered the topics of the security issues in mass public transport and how the sense of security is a key factor for users. It was followed by a detailed presentation of how the security is managed in Barcelona's public transport.

The event was closed with a project summary of the scientific findings and conclusions and a short demonstration of the project application tool.

During the whole event, the interaction between the audience and the speakers was dynamic and the panellist answered many questions and topics presented by the attendees. Many of these attendees showed their interest in the project, asked for further information about it and some of them were really interested in an extended demonstration of the project results.

Overall, the event was a great opportunity for dissemination and to show a good amount of the work done in community building and how it helped the project to develop and obtain results.

8. Conclusions

The work done in the stakeholders' panels has been essential during all the stages of the project. Since the beginning of the project, the panels have helped to define the requirements and scenarios of the case studies, to validate the models developed within the project (praised by their technical academic rigour) and to evaluate the results: a coherent and efficient set of instruments integrated in a clear and useful toolkit.

During all these stages, several meetings, conference calls, workshops and evaluation sessions have been held with the different stakeholders: gathering feedback, implementing iterative changes and producing a final result. This final result has been considered, with some calibration, as an effective decision-support tool for security policy-makers.

The major stakeholders' event, the SECONOMICS Summit, gathered together the main stakeholders from each case study and served both as a joint action and as a big dissemination opportunity bringing common conclusions and reaching further audiences.



All these activities have greatly helped the development of the final outcomes of the project, such as the software toolkit that integrates the core models in a user-friendly application or the good practises and methods on how scientific models can be used to develop evidence-based security policies. These results have been positively evaluated by all the involved stakeholders and have a great exploitation potential.

REFERENCES

- [1] D9.2 Users' panel definition and strategy - Silvia Castellvi (2012).
- [2] D9.8 First Stakeholders' panel report - Iván Zaldívar (2013)
- [3] D1.3 Airport Requirements final version - A. Tedeschi (2013).
- [4] International Civil Aviation Organization (<http://www.icao.int/Pages/default.aspx>).
- [5] D2.3 National Grid Requirements final version - Raminder Ruprai (2013).
- [6] D3.3 Urban Public Transport Requirements final version - R. Munné, M. Pellot (2013).
- [7] D9.14 Public_engagement_forum_workshops - Belén Gallego (2014)