SECONOMICS

Socio-economics meets Security

SECONOMICS synthesizes sociological, economic and security science into a usable, concrete, actionable knowledge for policy makers and social planners responsible for citizen's security

Issue 3 - Jun 2014

In this Issue:

Università degli Studi di Trento
DeepBlue consulting&research
Fraunhofer
Universidad Rey Juan Carlos
University of Aberdeen
Durham University
Transports Metropolitans de Barcelona
Atos
SecureNOK
SOU Institute of Sociology of the Academy of Sciences of the Czech Republic
nationalgrid
Anadolu University

www.seconomicsproject.eu

Anadolu University Workshop

The dissemination and validation workshop (M25) for airport security studies was performed at Anadolu University Workshop, 27-28th of February 2014. The workshop consisted of two sessions:

1. General SECONOMICS project and WP1 and WP4 studies presentations related to security perception at 27th February,

2. Focused presentations of WP1 scenarios and models on airport security and discussions at 28th February.

AU Workshop Objectives

The workshop objectives were:

1. Sharing information about SECONOMICS project studies with the stakeholders who are high level professionals about Airport and ATM security,

2. Putting together the stakeholders ideas about project scenarios, models and outputs by discussing on the provided data of WPs.

Participants

Anadolu University invited Turkish and South Eastern European professionals of airport security who can contribute to SECONOMICS studies because of their high-level knowledge and experiences as stakeholders. The workshop participants were mainly from Turkish civil aviation environment - professionals from European Commission, Turkish CAA-DGCA (Directorate of General Civil Aviation), Turkish ANSP-DHMI (which is responsible for all state airports), Airliners, Sabiha Gokcen (Istanbul) airport, Air Traffic Controller's Association (TATCA), researchers and project experts from Anadolu University.

Presentations

Project partners, guest speakers and the DGCA airport security representative performed the workshop presentations. Presentations can be summarized as follows:

1. Presentation of Project overview: this presentation was aimed to give general information about SECONOMICS project objectives and case studies specially in the airport security domain.

2. Presentation of ATM Security in Single European Sky: An EC expert emphasized the importance of ATM security in the European region and its regulatory framework, including EC and Eurocontrol regulations.

3. Presentation of Security Perception: AU and ISASCR made a survey and media research separately about security perception and combined meaningful data together, specially those related to security measurements in the airports. Partners also collaborated with DBL in an online research about security perception around Europe.

4. Presentation of Human Factors in Airport Security: A Human factors expert presented the important points which affects airport security operations performance. The security culture can be seen as a solution for efficiency of security operations. The security culture which is shared from top to down in the security and airport operation organizations is very important to invest on the security decisions and training of

human resources, and also for reducing costs for operators and airport users.

5. Presentation of Scenarios and Models: The scenarios and modeling of cyberthreats and attacks to tower focused on the impact levels and adversarial risk analysis and affective airport security regulations modeling.

6. Presentation of DGCA Recent Developments: DGCA presentation pointed out some developments about new regulations and airport security. DGCA focused on the training of airport security personnel to increase performance of security operations as an efficient investment on human resources.

Discussions

The participants were highly involved into all workshop sessions and contributed by asking questions and participating into discussions. The scenarios and modeling about airport security were found meaningful considering ATM operations in the center of all airport operations. The main points are listed below:

1. Security operations for users and airport operators. The airport security operations and its standardizations for everyone in the airport environment should be optimized to reduce costs. The specified security operations and regulations can be generated taking into account the capacity constraints for all users and operators in the airports.

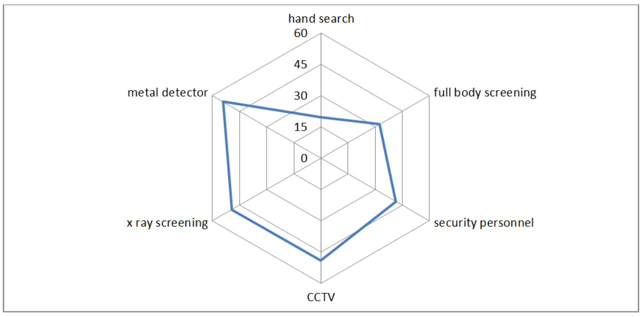
2. The security management activities can be seen as important as airport safety management activities and also both sectors should collaborate and be coordinated. Specially ATM, security is very sensitive to interact with flight safety and its impact level should be considered in order to its high social and economic cost. The security incident reporting data should be considered as the most important inputs for risk analysis and applying adversarial modeling.

3. Establishing security culture in airport operations can be seen as a long term solution to optimize the perception on security operations for all users and operators.

Ugŭr Turhan,
Alessandra Tedeschi

Case Study of Salience of Security measures: Acceptance of Airport Security

In this case study we focused on positive and negative salience of security measures as well as on perceived (subjective) setbacks of security measures[1]. First let us look at the general salience of security measures (the analysis is based on passenger's indication of security measures as important during security procedure, Figure 1). Among the security procedures, six general salience clusters can be identified, first the most salient security measures – led by metal detector (over 54 %), followed by X ray screening and CCTV; secondly, medium salience of security personnel (over 41 %) and full body screening (i.e. use of 3D body scanner); and low salience of hand search (almost 20%).



Note: N= 869
Source: Anadolu University

Figure 1 – General salience of security procedures (in per cent)

In the analysis of this question, we find significant differences based on socio-demographic variables such as age (passengers between 20 and 40 years of age are viewing security measures as more salient), gender (male passengers tend to view security measures as more salient, as compared to their female counterparts), religion (Christian and Muslim passengers are on average more sensitive to security measures than passengers belonging to other religion or no religion) and education (the higher the education, the higher salience of security measures).

In terms of negative salience (based on passengers' subjective evaluation of security measures as disturbing), three clusters of negative salience can be identified – high negative salience of hand search (almost 51 %) followed by full body screening (39 %); medium negative salience of X-ray screening (more than 17 %) and security personnel (16,5 %); and low negative salience of metal detector (9 %) and CCTV (almost 5 %).

Looking at the clusters of negative salience, it is clear that the degree of negative salience reflects the degree of perceived intrusion into personal and even physical sphere of passengers – the most negative being hand search presuming physical contact between passenger and security personnel, followed by screening by machine (viewed as more impersonal, however clear distinction is between 3D body scanner which has more than double the negative salience of X-ray screening), to a relative high acceptance (low negative salience) of non-contact security measures such as CCTV and metal detector.

In this respect, negative salience is significantly influenced by cultural differences – different cultures have diverse conceptions of private sphere and of the body (Moran et al 2007). In terms of socio demographics, similar patterns as in general salience can be found in the case of negative salience. Like in general salience we find significant differences based on socio-demographic variables such as age (passengers between 20 and 40 years of age expressed stronger negative salience than their younger and older counterparts),

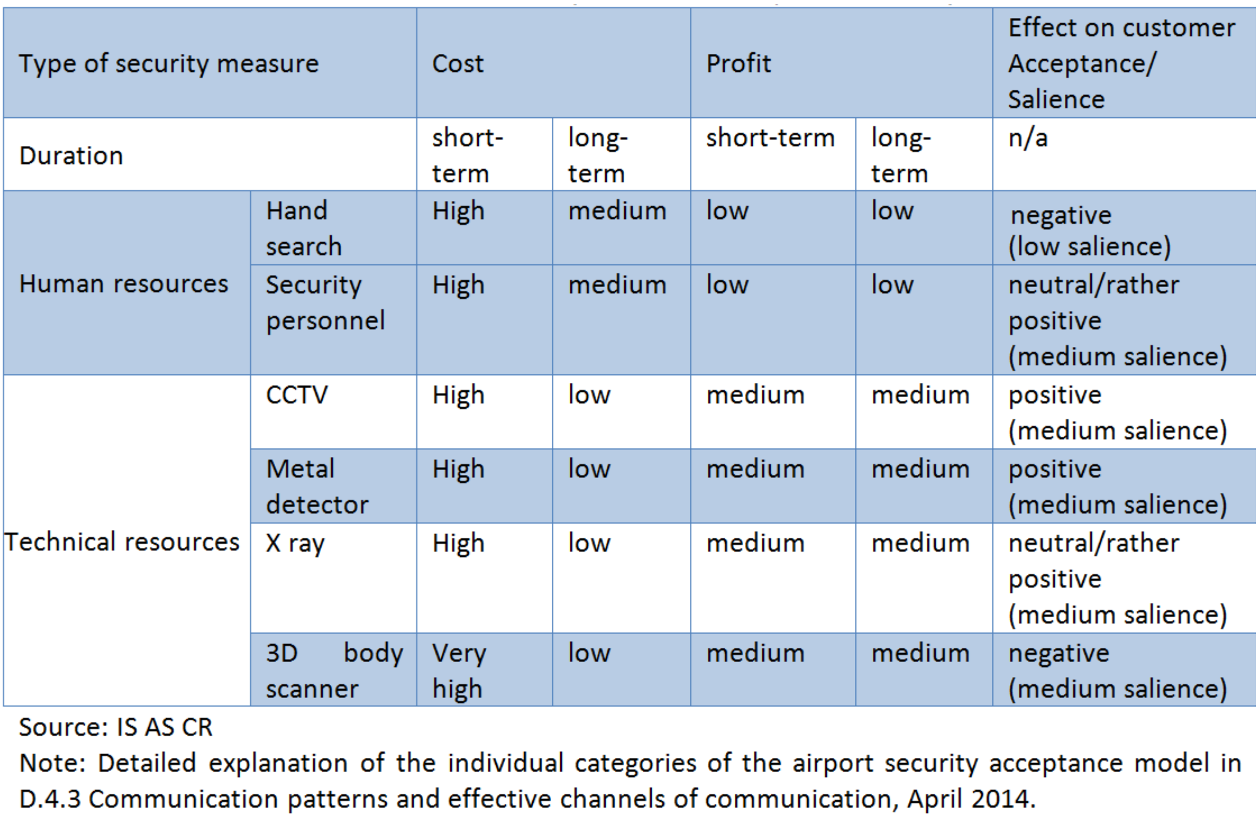
[1] Survey has been developed and put into practice by academics from the Faculties of Aeronautics, Anadolu University, Eskisehir, Turkey, and coordinated and performed by Dr. Nalan Ergun, Birsen Acikel and Dr. Ugur Turhan.

gender (male passengers tend to view most security measures as more negatively salient, as compared to their female counterparts, with the exception of full body screening and hand search where female passengers show higher negative salience), religion (Christian and to lesser degree Muslim passengers express on average more negative salience than passengers belonging to other religion or with no religion) and education (the higher the education, the higher the negative salience of security measures expressed by passenger).

These results hint at the need of airport authorities to consider passengers basic socio-demographic characteristics in order to successfully implement and perform security measures.

Model validation

At the airport models validation workshop held at the Anadolu University in February 2014, the model (Table 1) was introduced to the participants, who were asked to assess it in general (usability) as well as the values of the individual categories given their experience and background. In total ten interviewees provided detailed feedback, whose analysis can be summarised as follows.



Type of security measure		Cost		Profit		Effect on customer Acceptance/ Salience
Duration		short-term	long-term	short-term	long-term	n/a
Human resources	Hand search	High	medium	low	low	negative (low salience)
	Security personnel	High	medium	low	low	neutral/rather positive (medium salience)
Technical resources	CCTV	High	low	medium	medium	positive (medium salience)
	Metal detector	High	low	medium	medium	positive (medium salience)
	X ray	High	low	medium	medium	neutral/rather positive (medium salience)
	3D body scanner	Very high	low	medium	medium	negative (medium salience)

Source: IS AS CR

Note: Detailed explanation of the individual categories of the airport security acceptance model in D.4.3 Communication patterns and effective channels of communication, April 2014.

Table 1 – Model based on the effects of security measures in airport case study

In general, a difference can be observed between the assessment of the costs by the research team and by the interviewees. The value medium assigned by the interviewees to the short-term cost categories of hand search, security personnel, CCTV and metal detector, can be explained by the fact that compared to the general airport costs the above mentioned categories do not represent high expenditure. As for the value low assigned to long-term cost of X-ray and 3D body scanner, the difference is explained by similar justification as above and by the fact that the technology used has relatively low maintenance costs compared to other technologies employed in the airports.

Similarly to the comparison between conceptual model and validation of costs, the validation of profit shows variation between conceptual model and perception of airport security experts. The short-term profits of security personnel are perceived as medium by the experts, whilst being seen as low in the model and in turn, CCTV cameras and 3D body scanner short-term profits are viewed as low by the experts. In a long term the experts in the validation assigned high profits to metal detector as well as X- ray, and medium profit to security personnel, CCTV and 3D body scanner.

Last category compared is the salience of the individual security measures. This is the most important category in the SECONOMICS research on perception and acceptance of airport security. In the validation, the feedback of airport security experts was very positive and salience of security measures, which encompasses passengers' attitudes, was seen as both novel and beneficial for example in terms of future planning of security cost allocation.

In Table 2, we clearly see that unlike in the categories of costs and profit, the salience

	salience	model validation
CCTV cameras	positive	positive
metal detector	positive	positive
security personnel	neutral	neutral
X- ray screening	neutral	positive
full body screening	negative	negative
hand search	negative	negative

Source: ISAS CR, data Anadolu airport Survey and SECONOMICS validation workshop

Table 2 – Comparing salience in conceptual model, survey findings and validation

conceptually modelled and measured in Anadolu survey shows high degree of similarity with the opinion of experts. The exception is X-ray screening, whose salience is perceived as positive by the airport security experts during the validation but as neutral by the passengers in the Anadolu survey. Both our analysis and model validation categorise the metal detector and CCTV cameras as positive; security personnel (as neutral) and full body screening (3D body scanner) and hand search (as negative).

To conclude, the case study presented here – airport security- emphasizes the need for the decision-makers to consider existing and emerging threats, actual and perceived security, range of measures adopted to avoid these, provision of good and reliable services before taking the decision on acquiring certain security measure. Security costs as well as sociological impacts of adopted measures and policy decisions should be considered while taking into account public opinion reactions. Special attention should be paid to salience of security measures and cultural diversity which has an effect on salience.

As for the application of the model to the airport case, based on Anadolu Passenger Survey data analysis, it showed that both general salience and negative salience of security measures varies – hand search and full body screening show highest negative salience, whilst X-ray screening is significantly more accepted. It is therefore important for airport authorities to include the salience of security measures, and in particular the negative salience in their consideration of acquisition of security technology (along the cost and benefit analysis) and training of security personnel.

Petra Guasti

SECONOMICS
3. Media Analysis 2010 - 2013
The articles analysed in the study are all drawn from the period between January 2010 and April 2013.
Each article was sourced from the two most circulated quality dailies (i.e. mainstream newspapers) in the following countries:
the old and the new EU member states of the Czech Republic, Germany, Italy, Poland, Slovakia, Spain, the UK;
as well as non-EU member states important in either shaping the global discussions of the selected issues (the USA), or
key in providing relevant cultural diversity (Turkey and Mexico).
ANADOLU ÜNİVERSİTESİ
SECONOMICS

Participatory Interviews in the Airport Case Study Validation Activities

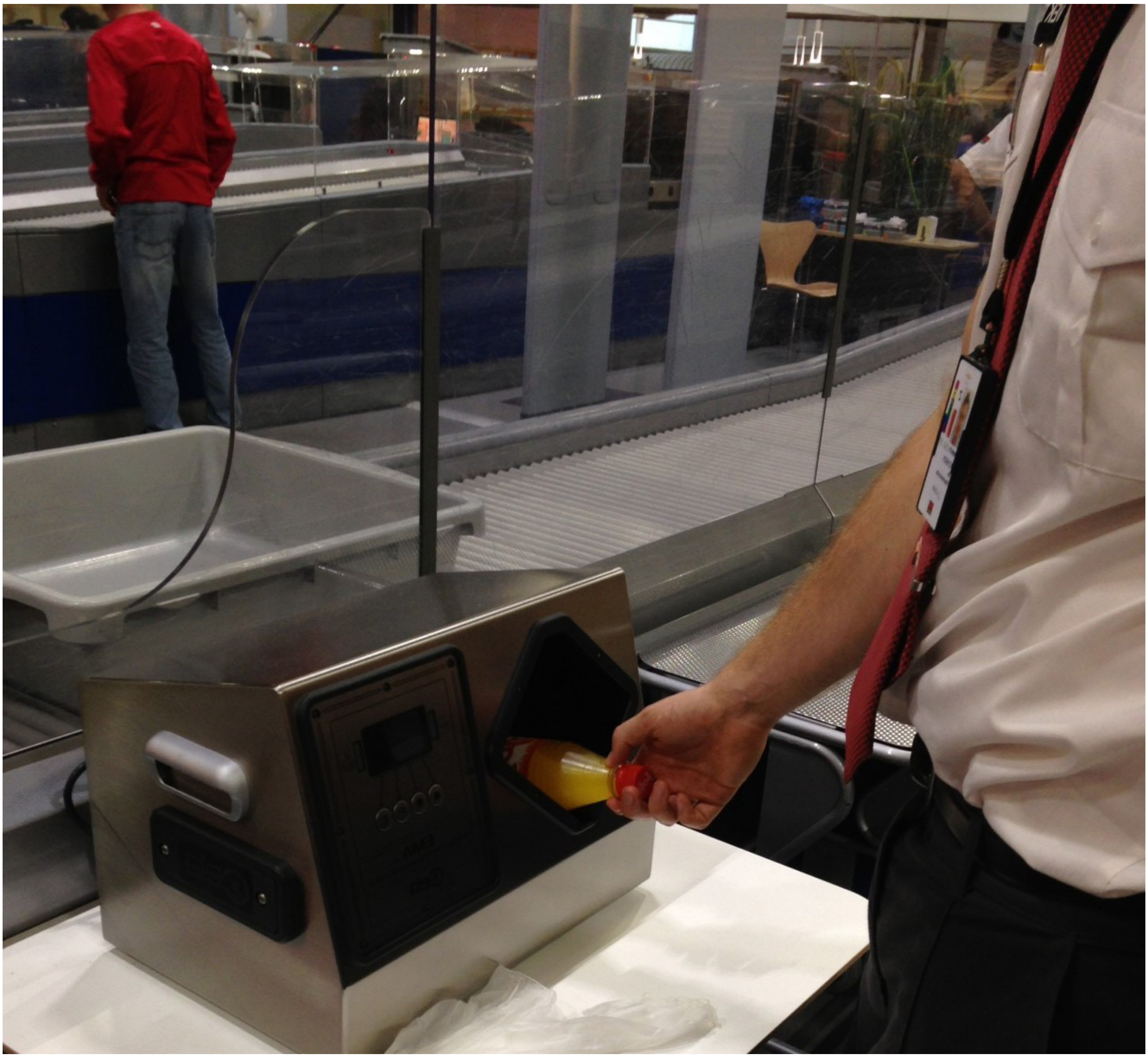
During the last period, validation activities of SECONOMICS have been supported by a variety of experimental methods. Particularly in WP6, validation of the economic models has been conducted through a series of participatory interviews with high-level representatives of the airport domain. In the three Validation Workshops at Falconara airport in Italy (September 2013) and Anadolu Airport in Turkey (November 2013 and February 2014), more than 15 high-level airport domain experts and stakeholders including airport security managers, air navigation service providers, private airport security contractors and government regulators have participated in focused interviews with the aim of obtaining broad as well as detailed knowledge of the current environment and issues in the airport security domain, and collecting enriched feedback and comments on the models developed in WP6.

A semi-structured interview technique, which is designed to use open-ended questions, has been employed. This allowed covering a wide array of issues and pursuing new ideas that emerge during the interview. Furthermore, the interviews made it possible to obtain not only factual data but also revealed attitudes and preferences of the participants, and to gain a deeper insight on the epistemological framework shaping their perception in reference to security related issues. The sampling for the interviews had been set in advance with the support of DBL and Anadolu partners. Interviews lasted approximately 30-40 minutes and sometimes a Turkish native speaker attended it. Moreover, interviews have been audio recorded with the permission of the interviewees and in parallel hand notes have been taken during the conversation, to collect feeling, perceptions and preliminary reflections. Audio records have then been literally transcribed and analyzed through thematic analysis.

Particularly, starting from efficiency, costs and social acceptance of different security measures, the interviewers were able to identify the tendencies driving the decisions taken by the interviewees with respect to the current security regulatory approach. A general opinion expressed by the airport security managers revealed that in a certain situation a security regulation mandated by the regulator does not fit properly with the specific airport needs, and that security regulatory rules and funding mechanisms should be designed to make an airport spend optimal security expenditures. A developed model based on the interviews therefore focused on the situation of the current aviation security regulations and policies, and paid a specific attention to identifying socially optimal combinations of security regulatory mechanisms (i.e., customized vs. uniform) and financial rules (i.e., centralized vs. decentralized) for different types of aviation networks.

Another knowledge we have obtained from the interviews is the detailed information and perspective on the structure of the security duties and responsibilities and the relationship between the actors involved in security tasks. The interview results indicated that principal-agent theory can be used to frame the relationship between the different security actors in relation to their strategic decisions. Incentive strategies, insourcing vs. outsourcing decisions as well as contractual relationships between the security actors have been identified and were included in the models for analyzing a principal-agent problem.

Woohyun Shim,
Martina de Gramatica



Critical National Infrastructure Case Study

Unlike the cases of airports, air traffic management and urban public transport, the public in general are less aware of critical national infrastructure or CNI that society relies upon. Whilst society relies on and uses CNI everyday, few understand its facets and intricacies and even fewer consider the information and cyber security aspects of CNI.

For the SECONOMICS CNI case study, the project has been focusing on the UK's Electricity Transmission Grid, owned and operated by National Grid. In this article we:

- Give a background to the National Grid company and the different infrastructures it operates globally
- Present an overview of Electricity Transmission in the UK
- Discuss the key challenge that the SECONOMICS research is hoping to answer
- Give some highlights of the CNI Validation Workshops.

Background to National Grid

National Grid plc is a British multinational electricity and gas utility company whose business activities are in the United Kingdom (UK) and in the North-Eastern United States of America (US).

In the UK, National Grid manages and operates both the electricity and gas transmission networks for the majority of the country. This includes England, Wales and Scotland. National Grid owns the transmission infrastructure for gas and electricity but only in England, Wales and Northern Ireland. In addition, the company owns and operates the distribution of gas in a number of regions of the UK. However, National Grid does not manage the distribution of electricity.

In the UK, National Grid employees approximately 10,000 people working across England and Wales. This includes the 24/7/365 control centres for electricity and gas transmission.

In the US, the structure of the energy and utilities market is somewhat different to the UK. As such National Grid own and are responsible for the generation, transmission and distribution of electricity in the following states of the North-Eastern US: upstate New York, Massachusetts, Rhode Island and New Hampshire. The company supplies electricity to over 3.4 million end-user customers. For gas, National Grid own and operate gas networks in the following states of the North-Eastern US: upstate New York (including New York City), Massachusetts, Rhode Island and New Hampshire. The company delivers gas to approximately 3.5 million customers in these states. National Grid has approximately 18,000 employees across the North-Eastern US.

Electricity Transmission in the UK

The focus of National Grid's input into SECONOMICS, and WP2 in particular, has been the UK electricity transmission network, also referred to as 'the grid'. The infrastructure that supports an electricity transmission grid consists of the following elements:

- Generators of electricity i.e. coal, gas, nuclear, solar, wind (etc.) power stations

- Distributors of electricity (the customers) i.e. those organisations that distribute electricity in a local/regional area
- The 'highway' of high-voltage electrical wiring that connects generators to the distributors
- Tele protection system to safeguard the public when transmission lines are damaged
- The data highway that travels with the power cables which provide voice and data, such as demand, supply, frequency etc., from the generators and distributors
- The Supervisory Control and Data Acquisition (SCADA) systems that take the data feeds and balances the electrical transmission grid through its links to all the generators and distributors.

To understand electricity transmission, it is useful to see how the elements above connect with each other in the wider picture. Figure 1, below, shows the full lifecycle of electricity from generation to distributor substation down to residential consumers. This diagram takes into account the elements described above and the scope of National Grid's responsibility is shown in part 'B Transmission'.

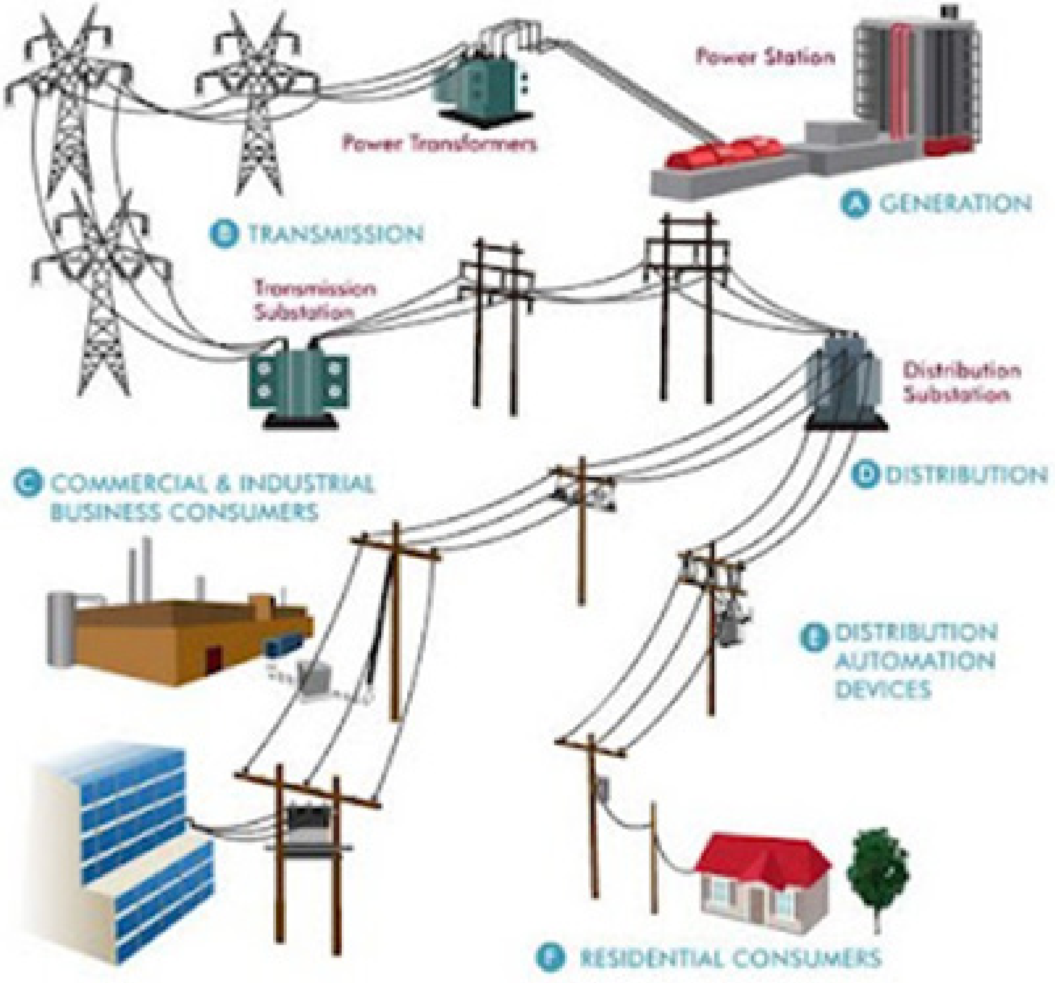


Figure 1 – Complete lifecycle of electricity delivery in the UK

National Grid's role within the wider picture of electricity delivery is to ensure that the demand of electricity by the distributors is met by the supply of electricity by the generation companies. To achieve this National Grid has to both manage and balance the grid at all times.

Managing the Grid

The grid is critical to the UK and National Grid has strived to ensure its resilience and availability. As a result, for each and every end user of electricity there are a number of transmission lines that can be used to service them. This allows for lines and pylons (towers) to be maintained, replaced and/or relocated without any interruption in the supply of electricity.

Managing the grid involves knowing which transmission lines are operational, their maximum load capacity, when they are due for maintenance work and if they are in immediate need of maintenance work. With this information, the control centres can determine which transmissions lines to take out of action for the relevant maintenance and where and how much electricity load can be spread across the rest of the network.

Balancing the Grid

For any specified time period National Grid needs to ensure that supply of electricity is meeting demand. The way in which this is done accurately is to view the frequency of the network. All generators output electricity as alternating current with a frequency of 50Hz. If supply is exactly meeting demand the frequency remains at 50Hz. However, if demand increases this causes extra load to be put on each generator and the frequency at each generator, and thus the entire network drops. On the other hand if demand falls, the load on each generator drops and the frequency of the network rises. It is the frequency of the network that the control room monitors. If the frequency of the system can be kept within tight limits then the network can be considered balanced. In the UK the acceptable limits of the frequency of the network is between 49.5 Hz and 50.5 Hz.

The frequency control algorithms and mechanisms decide when to increase or decrease the output of electricity at the different generation sites in order to balance the network. For example if frequency of the system starts to fall below 50Hz this shows demand is outstripping supply. Therefore at the pre-determined trigger point the frequency system will ask for increased output from the appropriate generators, which in turn will increase the frequency back to 50Hz.

SCADA Network

To effectively manage and balance the grid a physical network of fibre optic cables connects the electricity control room systems and the operators with substations, generators and interconnectors. This physical network can be used to exchange electronic information between them via technologies and protocols such as Internet Protocol (IP), Multiprotocol Label Switching (MPLS), telephony and facsimile.

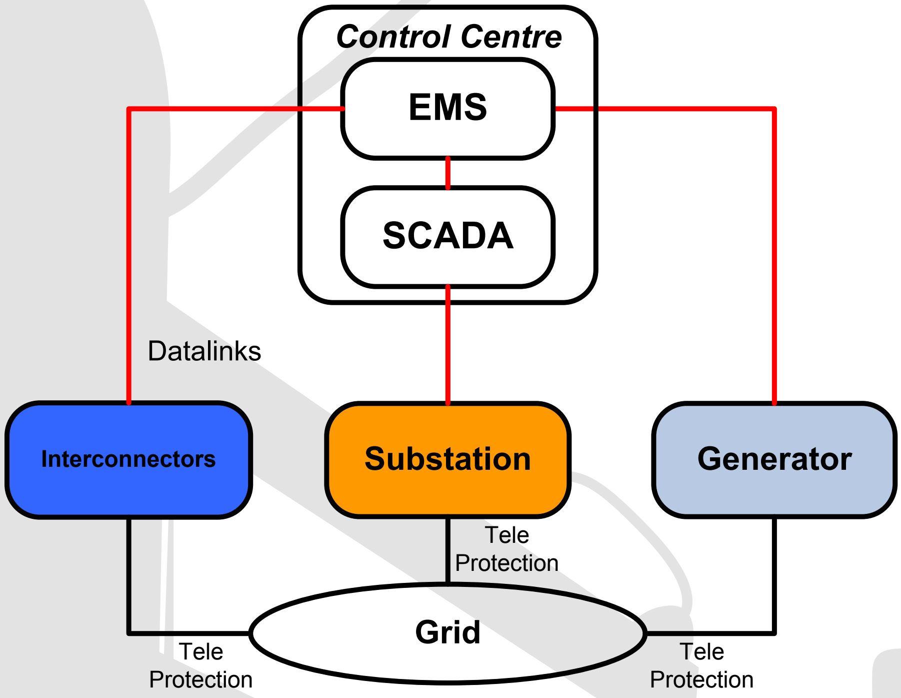


Figure 2 – Data links between the Control Centres, Interconnectors, Generators and Substations

Figure 2 shows the data links between the control centres and the interconnectors, generators and substations. The black lines between the interconnectors, generators and substations denote the actual power lines that connect these entities. Tele-protection systems are in place for safety across the high voltage power lines to stop live wires coming into to contact with commercial buildings, homes, vehicles and people. This will be discussed further in Security Scenarios section.

The red lines denote the fibre-optic data links that connect the entities to the control centre, specifically the Electricity Management System (EMS), through a front-end processing unit and a SCADA system interacts with the electricity transmission substations. In addition, there are interconnectors, distributers and generators linked to the balancing mechanism which determine demand forecasts and the electricity reserve. This is also discussed in the Security Scenarios section.

Broadly, the information exchanges required from the interconnectors, distribution networks and generators is to balance the electricity across the grid, whilst the SCADA system monitors and manages the grid infrastructure.

The Key Challenge

As National Grid operates electricity transmission networks in two different jurisdictions (UK and US) they have to comply with two different regulatory structures. In the UK, National Grid operates in a risks/principles-based environment whereas, in the US, National Grid operates in a rules-based environment. This is shown diagrammatically in Figure 3 below.

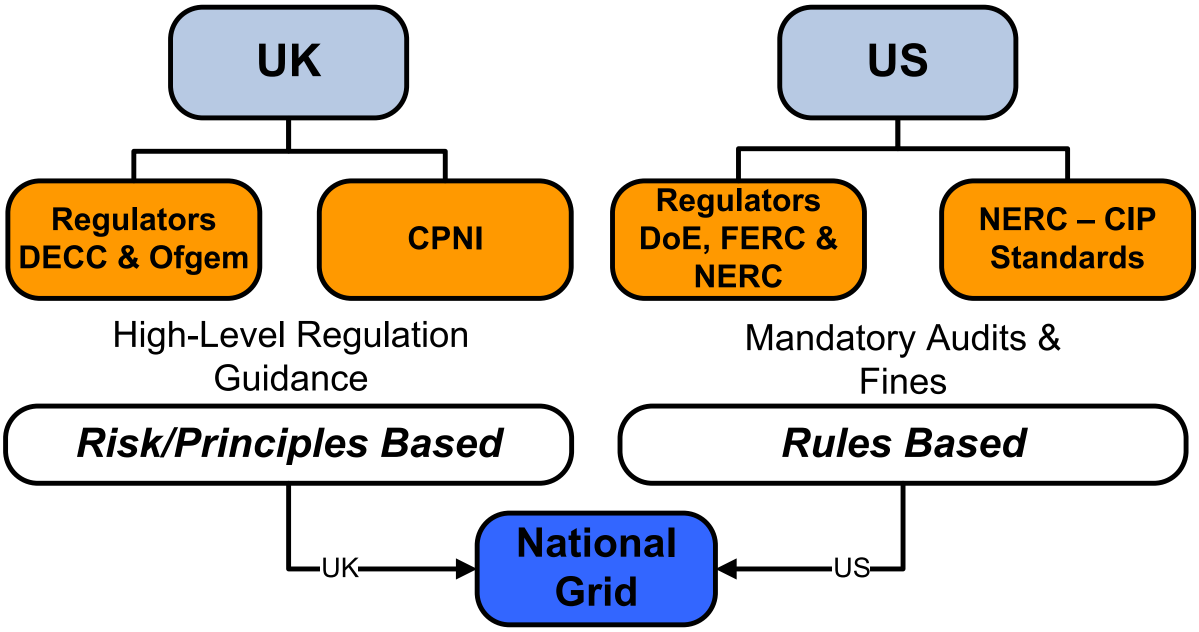


Figure 3 – National Grid Regulation in the US and UK

We have shown that the largest potential cyber security impact results when the integrity of the overall Electricity Management System is compromised. Manipulating the data being fed into and from the SCADA system, within the Electricity Management System, has the potential to cause significant power outages across the country or, in the worst case, a national black out. The comprehensive threat assessment also identified the various threat actors that could be motivated to cause such an event. Numerous other threats and risks were presented with the potential to impact the confidentiality and availability of the systems and data within National Grid as a CNI operator.

Given the potential impact that information and cyber security risks present to Electricity Transmission systems, it is essential that these risks are mitigated. However, such risks are not specific to Electricity Transmission and are present in other CNI such as a power generation sites or electricity distribution networks. Outside of electricity delivery, gas transmission/distribution, water treatment and delivery, telephone/broadband infrastructure and transport infrastructure are also susceptible to these security risks and can also be considered CNI.

Given the potential security impacts for CNI providers in particular, government has a responsibility on behalf of society to ensure that the providers protect the critical systems and services that are essential to the nation. From a governmental regulator perspective, their key concern is how best to ensure 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?

This is the key question that the CNI case study of the SECONOMICS project is investigating, which is presented in the following infographic.

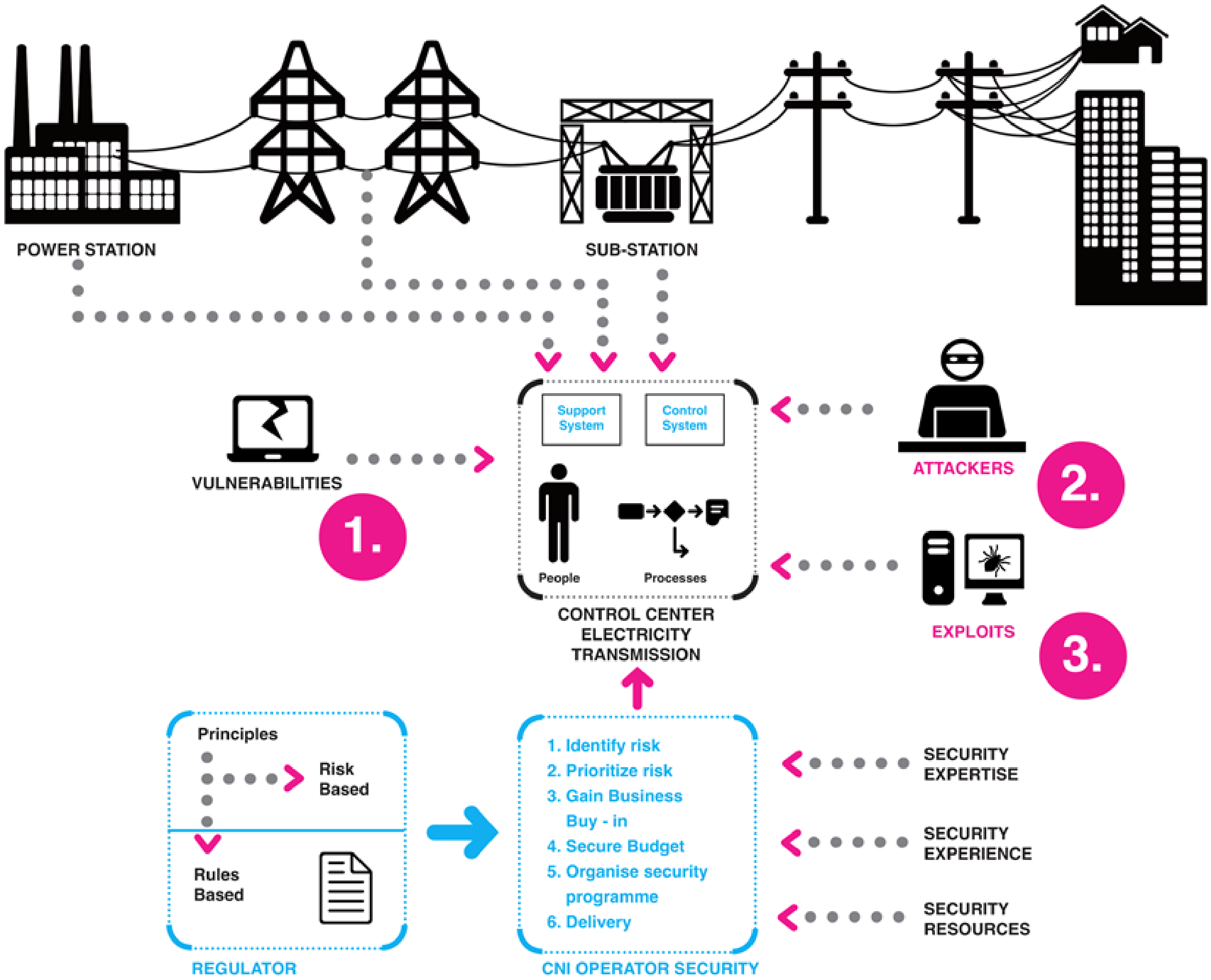


Figure 4 –Infographic: Securing CNI in an environment of vulnerabilities, attackers, exploits, constrained resources and different types of regulatory structures

Modelling Research

To attempt to answer the main question of measuring the effectiveness of a regulatory system/structure on a CNI operator, a number of models have been developed that look at this problem from slightly different view points in collaboration with the SECONOMICS project partners. These models are:

- An economics-based model that looks at the sustainability and resilience of the CNI holistically
- A systems-based model that looks at the agility of the CNI operator making specific decisions on security investment to mitigate security risks.

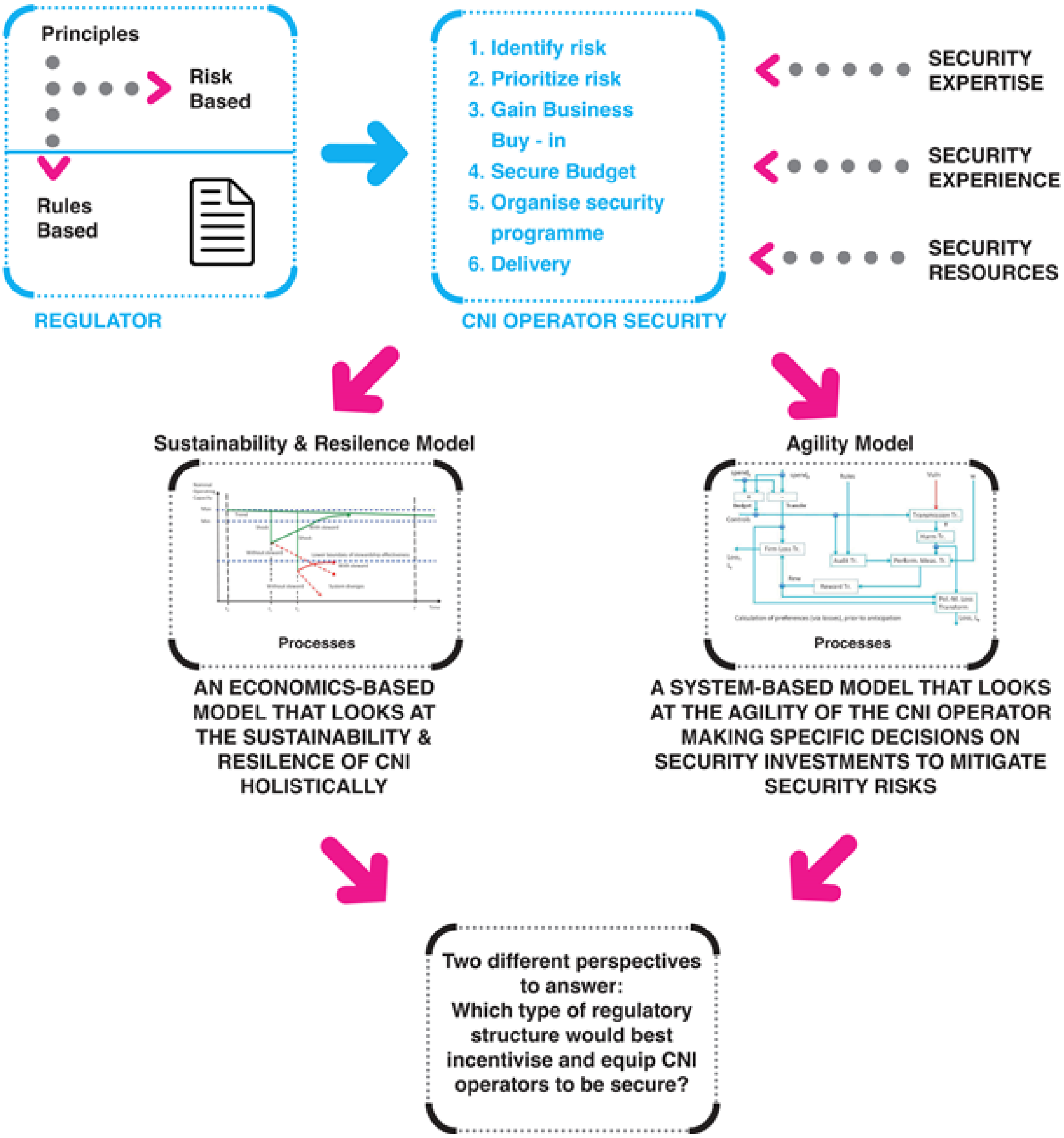

Principles
Risk Based
Rules Based
REGULATOR
1. Identify risk
2. Prioritize risk
3. Gain Business Buy - in
4. Secure Budget
5. Organise security programme
6. Delivery
CNI OPERATOR SECURITY
SECURITY EXPERTISE
SECURITY EXPERIENCE
SECURITY RESOURCES
Sustainability & Resilience Model
Processes
AN ECONOMICS-BASED MODEL THAT LOOKS AT THE SUSTAINABILITY & RESILENCE OF CNI HOLISTICALLY
Agility Model
Processes
A SYSTEM-BASED MODEL THAT LOOKS AT THE AGILITY OF THE CNI OPERATOR MAKING SPECIFIC DECISIONS ON SECURITY INVESTMENTS TO MITIGATE SECURITY RISKS
Two different perspectives to answer: Which type of regulatory structure would best incentivise and equip CNI operators to be secure?

Figure 5 – Infographic: How the Sustainability & Resilience and Agility models are answering the key question of the effectiveness of regulation.

Both models internalise the regulatory structure that is in place and how the CNI operator reacts to it and other events such as 'shocks' or cyber security attacks. In Figure 5 below, we show in an information graphic a depiction of how the two different models are being used to attempt to answer the key question from different stand points, and how the outcomes of these models will be brought together.

National Grid, along with the other SECONOMICS partners, is currently going through the validation workshops of the models with the key stakeholders for the CNI case study.

Raminder Ruprai

Public Transport dissemination activities

Professional conferences Rail BCN INNOVA at Rail BCN International Fair on Railway Industry

A dissemination presentation for professionals in the Railway sector was performed at Barcelona on 19th of November 2013. The presentation was done in the Rail BCN INNOVA framework, organized with the "Plataforma Tecnológica Ferroviaria Española (PTFE)" (Spanish Railway Technological Platform). This successful event is attended every year by professionals of the railway sector, especially urban, suburban and national railway operators.

2nd National Public Transport Workshop

A validation workshop for public transport security was performed in Barcelona, 19th of December 2014. This one-day workshop was focused on national level scope and it included the public transport security scenarios and needs; salience and acceptance of security measures and risk analysis modeling. After the presentation, a fruitful discussion within the experts took place.

The workshop participants were mainly professionals related to official security forces (Police) and other Spanish public transport operators.

The objectives were to share information about the SECONOMICS project with high level professionals on public transport security, and to understand the stakeholders' idea about project scenarios, models and outputs.

3rd International Public Transport Workshop (Karlsruhe 17/02/2014)

A validation workshop for public transport security was performed in Karlsruhe on 17th of February 2014. This one-day workshop was done within the 17th UITP's (International Public Transport Association) Security Commission. It was focused on international level scope and it included a review of the project; the public transport security scenarios and needs; salience and acceptance of security measures and risk analysis modeling. After the presentation, a fruitful discussion within the experts took place.

The workshop was attended by more than 25 participants -experts in security, mainly public transport operators.

The objectives were to share information about the SECONOMICS project with high level professionals on public transport security, and to understand the stakeholders' ideas about project scenarios, models and outputs.

SECONOMICS

Socio-economics
meets Security

Contact Info

Project Coordinator: Fabio Massacci
Università degli Studi di Trento

fabio.massacci@unitn.it

www.seconomicsproject.eu

@seconomics_eu

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285223