SECONOMICS

D7.2 – Critical infrastructure user requirements, covering Grid, transport and airport domains

T.S. Nguyen, S.H. Houmb (SNOK), A. Tedeschi (DBL), R. Ruprai (NGRID), R. Munné (ATOS), E. Chiarani, M. Angeli (UNITN), J. Williams (UNIABDN)

Document Number	D7.2
Document Title	Critical infrastructure user requirements, covering Grid, transport and airport domains
Version	1.0
Status	Final
Work Package	WP 7
Deliverable Type	Report
Contractual Date of Delivery	31.01.2013
Actual Date of Delivery	31.01.2013
Responsible Unit	SNOK
Contributors	DBL, NGRID, ATOS, UNITN, UNIABDN
Keyword List	Critical infrastructure, user requirements, cross-mission impacts
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. Julian Williams julian.williams@abdn.ac.uk
6	TMB Transports Metropolitans de Barcelona	FERROCARRIL METROPOLITA DE BARCELONA SA, Carrer 60 Zona Franca, 21-23, 08040, Barcelona, Spain http://www.tmb.cat/ca/home	Contact: Michael Pellot mpellot@tmb.cat
7	Atos	ATOS ORIGIN SOCIEDAD ANONIMA ESPANOLA, Calle Albarracin, 25, 28037, Madrid, Spain http://es.atos.net/es-es/	Contact: Silvia Castellvi Catala silvia.castellvi@atosresearch.eu
8	SECURENOK	SECURE-NOK AS, Professor Olav Hanssensvei, 7A, 4021, Stavanger, Norway Postadress: P.O. Box 8034, 4068, Stavanger, Norway http://www.securenok.com/	Contact: Siv Houmb sivhoumb@securenok.com
9	SOÚ Institute of Sociology AS CR	INSTITUTE OF SOCIOLOGY OF THE ACADEMY OF SCIENCES OF THE CZECH REPUBLIC PUBLIC RESEARCH INSTITUTION, Jilska 1, 11000, Praha 1, Czech Republic http://www.soc.cas.cz/	Contact: Dr Zdenka Mansfeldová zdenka.mansfeldova@soc.cas.cz
10	nationalgrid THE POWER OF ACTION	NATIONAL GRID ELECTRICITY TRANSMISSION PLC, The Strand, 1-3, WC2N 5EH, London, United Kingdom	Contact: Dr Ruprai Raminder Raminder.Ruprai@uk.ngrid.com
11	ANADOLU ÜNİVERSİTESİ	ANADOLU UNIVERSITY, SCHOOL OF CIVIL AVIATION Iki Eylul Kampusu, 26470, Eskisehir, Turkey	Contact: Nalan Ergun nergun@anadolu.edu.tr

Document change record

Version	Date	Status	Author (Unit)	Description
0.1	13/12/2012	Draft	S.H Houmb, T.S Nguyen (SNOK)	1st draft
0.2	17/12/2012	Draft	T.S Nguyen (SNOK)	Change section number; add content for sections 1, 2, 6, and 7.
0.3	21/12/2012	Draft	A. Tedeschi (DBL), R. Ruprai (NGRID), R. Munné (ATOS), T.S Nguyen (SNOK)	Modify sections 3-5 with comments from partners. 1st draft for internal scientific review and quality check.
0.4	04/01/2013	Draft	R. Ruprai (NGRID) E. Chiarani (UNITN)	Internal scientific review completed. 1st quality check completed.
0.5	14/01/2013	Draft	A. Tedeschi (DBL), R. Ruprai (NGRID), R. Munné (ATOS), T.S Nguyen (SNOK)	Address comments from the internal scientific review with inputs from WP1-3 partners.
0.6	16/01/2013	Draft	R. Ruprai (NGRID)	2nd internal scientific review completed.
0.7	18/01/2013	Draft	T.S Nguyen (SNOK)	Address 2nd internal scientific review comments. Final draft for scientific review and quality check.
0.8	24/01/2013	Draft	M. Angeli (UNITN)	Final quality check completed.
0.9	29/01/2013	Draft	J. Williams (UNIABDN)	Final scientific review completed.
1.0	30/01/2013	Final	T.S. Nguyen (SNOK)	Address comments from final scientific review. Final version for submission.

INDEX

Executive summary

SECONOMICS is a collaborative research project on the socio-economics of security focusing on both information and physical security. The project is driven by three industry case studies in critical infrastructure protection. The case studies apply to airport security (Anadolu airport case study), security of energy distribution (the UK's National Grid case study), and security of local and urban transport (Barcelona's urban transportation case study.)

The project's goal is to synthesize sociological, economic and security science into a usable, concrete, actionable framework and toolkit for policy makers and social planners responsible for citizen's security. This framework defines a socio-economic methodology that span across different domains, such as airport, Grid and urban transport, in order to support decision-making processes on the viability of security measures, taking into account the impact on citizens.

WP1, 2, and 3 of the project provide case study inputs while WP4, 5, and 6 develop project's technical results based on those inputs. WP7 and 8 will then integrate those results into the SECONOMICS framework and toolkit respectively.

WP7 has three main responsibilities: (i) gather user requirements from the case study domains: airport, Grid and transport; (ii) consolidate experience and results across the three case study domains: grid; and (iii) consolidate and generalize the SECONOMICS framework based on the project's technical results.

This deliverable addresses responsibilities (i) and (ii) of WP7 that gathers and consolidates case study security requirements from WP1, WP2, and WP3. We present policy decision-making needs in each case study and generalize cross-domain decision-making needs. This deliverable also discusses how the case studies help to addresses security and cross cutting missions of the SECONOMICS project.

1. Introduction

1.1. Scope of the Report

This D7.2 report is one of five deliverables in work package WP7 of the SECONOMICS project, which has a final goal to generalize the SECONOMICS framework. The list of deliverables in WP7 include:

- D7.1 - Validation plan;
- D7.2 - Critical infrastructure user requirements, covering Grid, transport and airport domains;
- D7.3 - SECONOMICS framework aggregation;
- D7.4 - Case study consolidation;
- D7.5 - SECONOMICS framework generalization.

This D7.2 deliverable gathers and consolidates user requirements from three case studies regarding airport security, security of the UK National Grid, and security of Barcelona urban transport system. We gather security requirements, elaborate possible stakeholders, and discuss security decision-making challenges in each case study.

As the three study domains have both common and distinct security challenges, results from one case study may be applicable to others to some extent. We, therefore, provide a discussion on cross-mission decision-making needs, which addresses common security challenges across domains.

The key issues that are addressed in this deliverables are:

- SECONOMICS security missions and how the case studies address them;
- The policy decision-making challenges in each case study;
- The cross-domain decision-making needs that are applicable for more than one case study.

This report and the other deliverables in WP7 will then be used to generalize the SECONOMICS framework.

1.2. Document Overview

The deliverable D7.2 is organized as follow:

- In Section 1 Introduction, we present scope of this report, which contains key issues covered in the report. We also provide an overview of this report and then briefly revisit the SECONOMICS project aims and expected results.
- Section 2 presents the security missions that the SECONOMICS project should address.
- Section 3, 4, and 5 focus on three case studies in WP1, 2, and 3 respectively. In each of these sections, we summarize security scenarios, threats and impacts in each case study. Further discussions of stakeholders and their interactions in each case study are also presented. Each section is concluded by decision challenges that the SECONOMICS project need to help the case study to address. These challenges are what the case studies expect to get out of the project.

- In Section 6, we generalize and discuss decision challenges across domains to form cross-domain decision challenges. Those are the common challenges for more than one domain. The challenges are also classified into different levels from the international level down to operational level and possibly to the end users of the CNI.
- In Section 7, we discuss how the case studies in SECONOMICS project help to address its six security missions. It shows that with input and requirements from existing case studies, the expected results from the project is able to address all security missions targeted in the project proposal.

1.3. Project Aims and Expected Results

The SECONOMICS project's goal is to synthesize sociological, economic and security science into a usable, concrete, actionable knowledge for policy makers and social planners responsible for citizen's security. To meet this goal, SECONOMICS is designed to deal with cross-domain and multi-perspective challenges, including policy, risk, economics and security.

The main objective of the SECONOMICS project is to develop innovative risk assessment techniques and tools that will support policy makers in security-related decisions by taking into account societal and economic factors. This is particularly challenging when considering both logical and physical security aspects and in different domains in a pan-European perspective.

The overall outputs of the project are twofold. First, the project will provide assessments of the future and emerging threats in the identified areas with rigorous modelling of the optimal mechanisms for mitigation within the policy domain. Second, and more crucially, the project will develop a generalized framework and a policy "toolkit" to assist decision makers in identifying and reacting coherently (within the appropriate social context) to future and emerging threats that may arrive long after the project has been completed. The practical relevance of the project technical results will be validated against three challenging domains: airport, Grid, and urban transport.

In summary, the expected outcomes of this SECONOMICS project include:

- A general socio-economic framework for security resource allocation which is relevant across various domains;
- A policy toolkit that facilitates such process to policy makers;
- Showcases of such framework and tool in relevant case studies, which may serve as best practice analysis that may replicated in other critical infrastructures;
- Putting into consideration the global risk governance process issues in relation with social perceptions and attitudes towards;
- Improvement of the process of identifying and assessing risks from an economical point of view;
- Improvement of the process of balancing security with policy, economics and other relevant constraints;
- Improvement of the process of quantifying positive and negative externalities.

The project's initial task is to identify concrete issues in security missions for the three case studies. After that, the project's R&D work-packages, i.e. WP4-6, characterize

threats and distillate socio-economic methodologies based on rigorous and well-developed methodologies from the social sciences, risk and operations research, and economics and systems models.

- WP4 identifies qualitative societal impact scenarios from future or emergent threats. Quantification of the social cost is made by contingent valuation;
- WP5 identifies the outcome space and associated risk measures. This work package also analyses threat environments, security measures, and their effectiveness;
- WP6 develops economic and system models of the policy interactions with the architecture of the physical and ICT system under threat. The work package also develops an optimal set of policy tools and control instruments designed to optimally deal with future or emergent threats, subject to social cost constraints.

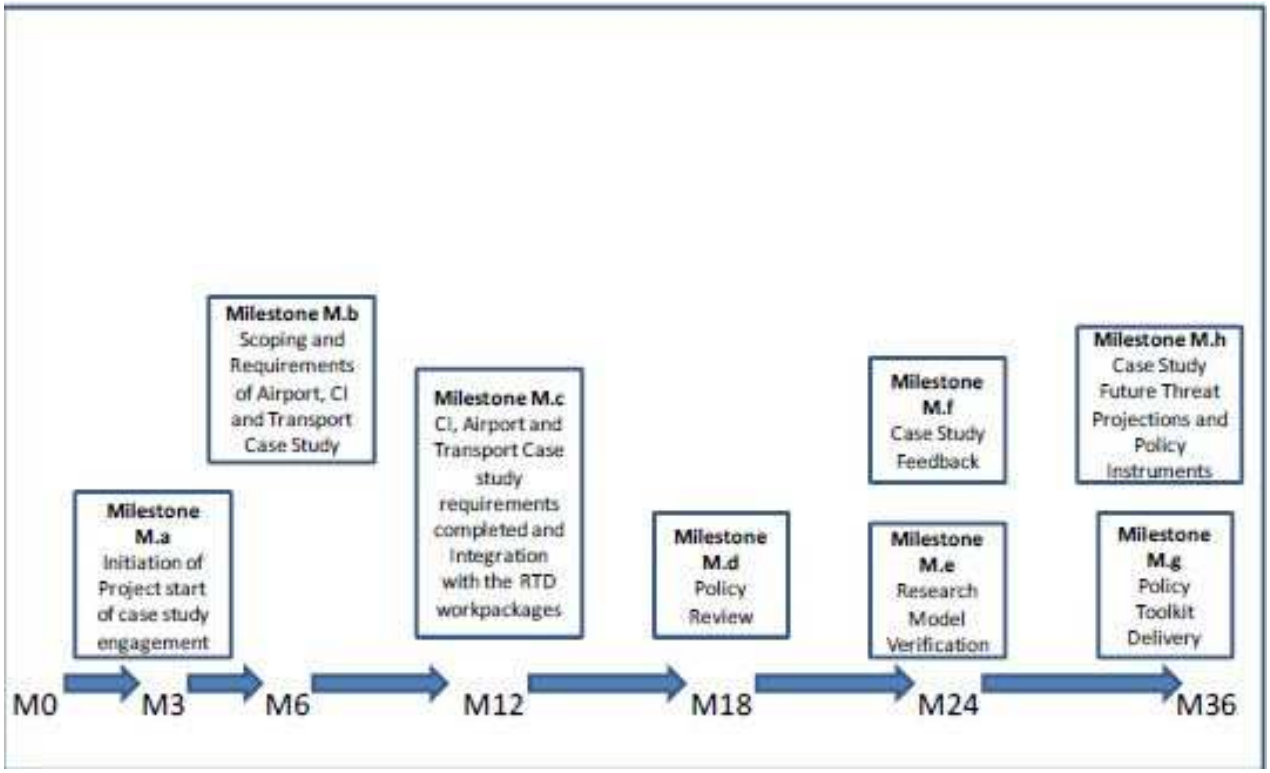

Figure 1 SECONOMICS Milestones and Expected Results

The final goals of this project is to provide a general framework and policy toolkit that is cross-mission and to provide guidance to decision makers on which types of legislative and regulatory instruments that are best suited to a particular emerging security threat. WP 7 and WP8 address these aspects of the development.

- WP7 will consolidate the results of the three case studies to cross-mission relevance results and will assist in consolidating validation assessment between WP4, WP5 and WP6;
- WP8 will provide a toolkit that maps research models either to collected or simulated data. The toolkit will be used in supporting the decision-making process.

1.4. Validation

As presented in deliverable D7.1, the validation plan of the SECONOMICS project contains three phases.

- Phase 1 - Stakeholders' operational needs identification – this is to identify the domain security stakeholders and policy makers involved in the validation process. It also defines the application scenarios and validation criteria;
- Phase 2 - Models validation – in this phase, iterative and incremental modelling activities will be carried out to evaluate both models' consistency and validity from an operational point of view and the modelling language expressiveness and completeness. Models will be presented and discussed with relevant stakeholders. They are then refined iteratively;
- Phase 3 - Framework and toolkit validation – a prototype evaluation will be used to steer the tool in the right direction in early stages of this phase. The validation will ensure that the final version of the tool satisfies users' needs expressed by validation criteria. Live trials will be set up whenever possible for the final validation.

The objective of D7.2 is to consolidate results from case studies in WP1, WP2, and WP3. It thus focuses on phase 1 of the validation plan, which applies to three case studies. In each of the corresponding case study section of this report, we will present a validation subsection and discuss if outputs from the case study work package meet the validation requirements.

2. Security Mission Impacts and Case Studies

The SECONOMICS project is framed around three case studies of security in airport (Anadolu airport, Turkey), critical national infrastructure (UK National Grid) and urban transport infrastructure (Barcelona underground network), driven by acknowledged industry leaders in their areas. All case study domains concern major critical services in modern society and have high requirements for security. This includes providing services to citizens as well as protecting the citizens against harmful actions. As resources are limited, it is also important to balance cost and security and to ensure a balanced security resource allocation.

SECONOMICS's goal is to provide a general socio-economic methodology to assist security decision-making processes. The methodology and its underlying process need to balance societal needs, the needs and risk perception of citizens, security requirements, economic perspectives and security policies on various levels. The tool-driven methodology will offer policy decision support that is generalized across various types of critical infrastructures. The outcomes of the project will be models, software tools and guidelines for policy makers.

The project aims to address security and cross cutting missions defined in the FP7 Security theme[1]. The security missions are:

1) Security of citizens;
2) Security of infrastructures and utilities;
3) Intelligent surveillance and border security;
4) Restoring security and safety in case of crisis.

The cross cutting missions are:

1) Security systems integration, interconnectivity and interoperability;
2) Security and society;
3) Security research coordination and structuring.

The project sits within the security research theme and addresses all security missions. It also addresses cross cutting mission 2 and 3, and some part mission 1.

We revisit the SECONOMICS missions in this section and will discuss how the project's case studies address these missions in Section 7.

Security mission 1 – Security of citizens - this mission concerns about civil protection and security threats affecting equipment and resources used by citizens, as well as protection against crime and terrorist attacks. Other important aspects are threat awareness, perception and detection. The key aspects of this mission are to identify and prevent security attacks against citizens and to prepare appropriate measures and response strategies in cases of undesired incidents. The SECONOMICS project addresses this mission through its three case study domains and with the development of a cross-mission policy decision framework where security of citizens is a core component.

Security mission 2 – Security of infrastructures and utilities – infrastructures are critical in a modern society and their efficient and continuous operations are crucial, both for

[1] http://cordis.europa.eu/fp7/security/about-security_en.html

business and for security and safety of citizens. This mission concerns with the protection of critical infrastructure and utilities in the European society. It includes all computerized supported critical infrastructures, such as the electricity grid, transportation systems and airports, which are the three case studies in the SECONOMICS project. The important goals are to identify, prevent, protect and react to security threats happened to these infrastructures.

Security mission 3 - Intelligent surveillance and border security – this mission concerns with the protection of borders, safe flow of citizens and measures in place to detect, identify and react to potential security hazards based on high-quality intelligent information. The airport security case study in WP1 addresses this mission directly. Border security is essential for ensuring security of the airport premises, as well as security of a nation and its citizens. International airports are important border control points and policies for border security and intelligent surveillance are of high importance. The SECONOMCS project will use the airport case study to extract general policy rules and best practices that can be of interest for other border control critical infrastructures, such as international trains, busses and boats.

Security mission 4 - Restoring security and safety in case of crisis - this mission concentrates on technologies used to provide an overview of and support for diverse emergency management operations such as civil protection, humanitarian aid and rescue tasks. Emphasis is on issues such as general organisational and operational preparedness to cope with security incident, crisis management, intervention in hostile environment, emergency humanitarian aid, and the management of the consequences and cascading effects of security incident. Policy decisions need to prepare, respond and recover from crisis. WP3 with the Barcelona urban public transport case study will focus on policy issues and decision process concerning the restoring of security and safety in crisis situations. The experience from WP3 will then be generalized and applied to the airport and GRID case studies (WP1 and WP2).

Cross cutting mission 1 - Security systems integration, interconnectivity and interoperability – this mission addresses the integration, interconnectivity and interoperability across various security systems. The SECONOMICS project addresses part of this mission by focusing on generalizing the SECONOMICS framework and on the interoperability between the components of the framework. The framework and toolbox will support standard interfaces and information exchange formats to enable an interchangeable module-based policy decision tool support.

Cross cutting mission 2 - Security and society – this mission concentrates on a multi-domain challenge of protecting the modern European society from security threats causing harm to citizens, infrastructure, nations or the European community. The three case studies all address essential European infrastructures. Transportation system is essential in ensuring secure flow of personnel and for protecting citizens. Airports are major border control entities with strict security demands and multi-level policy decision context. As the case study in WP2 shows, the electricity GRID is crucial to individual citizens, corporations, the government and society as a whole. At the same time, the electricity grid is vulnerable to threats and attacks. Power outage has large consequences for the industry, society and citizens, specifically in cold areas of Europe. Loss of power supply will have devastating consequences across Europe should security

attacks on the electricity grid be successful, or in case of shortage of availability of power resources.

Cross cutting mission 3 – Security research coordination and structuring – the project addresses this mission with a consortium of eleven partners from seven countries consisting of research institutions and SMEs.

3. Airport Security Case Study

With a large number of people passing through every day, airports are potential targets for terrorism and other forms of crime because of the high density of people co-located in a particular area. Similarly, the potential high death rate due to attacks on aircraft and the ability to use hijacked airplanes as dangerous weapons making aircrafts alluring targets for terrorism. In addition to a potential high death rate in successful aviation attacks, negative economic impacts of those attacks are very high as the attacks do not only have negative effects for airports and air carriers but also have negative effects to the regions where the airports located.

In order to prevent and mitigate potential aviation security threats, aviation security policies and countermeasures in general and those of airport security in particular need to be applied. Airport security refers to techniques and methods used in protecting passengers, staff, aircrafts that use airports as well as protecting airport facilities from accidental or intentional harms, crime and other threats.

WP1 of the SECONOMICS project focuses on airport security using Anadolu airport in Turkey as a case study. The key objective of WP1 is to steer the development of the decision-making tool in support for airport security. WP1 however also discusses other high level regulations that apply to all other airports.

This D7.2 report is based on deliverables D1.2 and D1.3 to consolidate security requirements for critical infrastructures in which airport is one of the case studies.

3.1. Airport Security Scenarios, Threats and Security Impacts

Deliverable D1.2 presents a number of security scenarios in the airport case study. Following the research questions provided by the project technical work packages, three security scenarios were finally selected and presented in deliverable D1.3. These include two high-level security scenarios for policy makers and one operational security scenario.

In this section, we briefly revisit those security scenarios and summarize airport security impacts of this case study. Further information and analysis about security scenarios and security requirements can be found in deliverable D1.2 and D1.3.

Airport Security Scenarios and Threats

The security in the airport case study can be categorized as high-level and locally operational security scenarios. While countermeasures for high-level security scenarios may require involvement of policy makers and regulators at different levels, local decision makers at the airport can decide those for operational level security scenarios.

- High-level security scenarios include:
    - Passenger-baggage security screening – this scenario merges and integrates passenger-baggage reconciliation and body scanner scenarios in deliverable D1.2. This scenario discusses security measures on passenger and baggage from check-in points at the departure airport to baggage reclaim at the arrival airport. This scenario also focuses on new technologies for

passenger check such as full body scanner and on passenger-baggage reconciliation procedure;
    - Training of airport personnel – training of airport personnel is crucial to guarantee aviation and airport security. There is no substitute for highly trained and qualified personnel because over-reliance on technology may leave passengers, crews, and airport personnel vulnerable to attacks. Nowadays, security training is a required component for all airport personnel, from airport security officers to truck drivers to custodians, with a need for unescorted access. Individuals are trained to recognize and act upon certain security breaches.
- An operational-level security scenario is:
    - Unlawful access to the air traffic control tower – in this scenario, intruders can penetrate and enter the air traffic control tower and take hold of air traffic controllers before or during the flight control operations. The intruders can use all radio and telephone communication aids in tower to pass their message.

All those security scenarios pose potential threats to the airport and aviation security if proper security measures are not deployed.

Security Impacts

Each scenario presented in the airport security case study has negative security impacts if intruders are successful in exploiting the security weaknesses.

- Passenger-baggage security screening – this group contains a large number of possible threats. The security impacts of threats in this group are very high because if any of the security requirements is violated, dangerous items can be passed to post-security areas and to the aircraft, which will cause dramatics consequences. After two famous terrorist incidents in 1985 and 1988[2], applying passenger-baggage reconciliation greatly reduces this type of threats though it does not prevent suicide bombers. A mandatory requirement of passenger-baggage reconciliation also causes flight delayed if the passenger cannot reach the boarding gate on time while their baggage is already checked in. That means beside security impacts, threats in this group also create negative economic impacts for the airport operators and air carriers;
- Personnel training – in addition to technical equipment and security procedures, the capability of airport security staff to identify potential intruders is very important. Hiring of unqualified security personnel greatly reduces the effectiveness of the whole security system. The role and impact of security training for airport personnel are critical;
- Unlawful access to the tower and interference to ATC operations – This incident has a very high security impact. It causes crisis for air traffic operations in the airfield and airspace and affects flight. Besides negative security impacts, the economic impact is also high as all flight operations are cancelled and/or delayed which causes huge economical loss for both traveling passengers and the airport itself.

[2] See deliverables 1.2 and 1.3 for more information.

3.2. Case Study Validation

According to deliverable D7.1, validations in the airport security case study fall into four categories:

- Selection of focus groups;
- Stakeholder interviews;
- Methodology evaluation;
- Walkthrough and tool live demo with stakeholders and policy makers.

By the end of Phase 1 of the SECONOMICS project, only the first two validation categories in the airport case study apply.

The security scenario identification and user requirements in the case study presented are chosen and developed based on a selection of and interviews with an expert group of airport stakeholders, including representatives of air navigation service provider (ANSP) security officers, aviation authority, airport management, airspace users and technology providers. The selection of expert groups and interviews guarantee that the selected scenarios and listed user requirements meet requirements from the project in general and meet validation criteria of D7.1 in particular.

Details about the involved stakeholders in airport security case study can be found in Section 3 “Stakeholders and Engagement Plan” of the deliverable D1.3.

3.3. Airport Security Stakeholders and Their Decisions

The ultimate purpose of airport security policies is to follow general or specific security guidelines to guarantee safety and smooth movement of travelling passengers, safety and efficient operations of airport facilities and its personnel, of aircrafts using the airport and of the national/regional security as a whole. However, those policies need to take into consideration available resources, e.g. human resources, available airport or regional/local financial budgets etc., as well as passenger convenience. Thus, certain specific security policies have to be compromised to meet other requirements.

There are a number of stakeholder groups involving the airport security. The distinctions between them depend on decisions they can make and how those decisions affect other groups. In generic sense, there are three large stakeholder groups: (i) the regulations making groups who can decide on high-level policies and regulations; (ii) the airport operation groups who can make low-level operational decisions; (iii) and the end user groups who can make individual decisions. They are different in motivations, and sometimes, benefits in making decisions. Some groups may contain subgroups, as the decision-making process is hierarchical.

From the top-down view, the stakeholders in the airport security case study can be placed in six distinctive levels. In the section below, we present the stakeholder levels and possible decisions they can make regarding airport security.

- International level such as ICAO - ICAO works together with national governments and key industry organizations to develop policies and standards with aviation security provisions disseminated in Annex 17 [1].

  - Regulate general security requirements for airside and airport perimeter (fences, walls, intrusion detection system, CCTV system, security lighting and patrols by guard forces);
  - Regulate general screening requirements for passengers and staff before granted access to security restricted areas;
  - Regulate screening requirements for passengers and baggage;
  - Regulate on-board security requirements for air carriers.
- European level such as EASA - EASA addresses ICAO standards and goes beyond them to increase safety and security of aviation in European region.
  - Regulate national aviation security program (NSP) requirements, which require air carriers, airport operators, handlers, and service providers to have security programs;
  - Impose one-stop security requirement within Europe;
  - Allow member states to adopt alternative security measures with adequate level of protection on the basis of local risk assessment at airports with specific characteristics;
  - Regulate security examination methods e.g. screening methods (x-ray, hand search, visual check etc.,), supplementary means of examination, and security control of supplies sold or used in security-restricted areas;
  - Impose security requirements for the air navigation services (ANS), air traffic management (ATM), communication, navigation and surveillance (CNS) assets and personnel;
  - Impose security requirements for air carriers.
- National level - each country has one civil aviation authority (CAA) to overlook all of its aviation issues, including aviation security. In addition to complying with requirements from ICAO and EASA, national regulators impose more details or additional requirements, including:
  - Impose requirements on training and development of NSP courses;
  - Regulate quality control requirements containing security surveys, security inspections and audits, and risk assessments;
  - Optionally, national regulators could impose security requirements in pre-security areas to reduce possible threats.
- Regional level
  - Protect airports as strategic facilities similar to those of power plants or train stations, for example by public police forces;
  - Decide about local laws and economic investments.
- Operational level – since many requirements from higher level regulatory bodies are general and instructive, it is up to each local entity to decide proper security measures. For example, in the US, TSA only sets minimal security standards at airports and provides some training to outside security officers from the state and local authorities[3]. Thus, the decision makers at each airport need to decide on proper security countermeasures.

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

- Provide detail and concrete technical security measures to mitigate threats;
- Decide which type of goods can be sold in post-security area so that it does not affect the airport security[4].

- Travelling passengers
  - Choose to continue their travels or to take other alternative options (choosing other airports or taking other means of transport);
  - Oppose to specific security measures, e.g. passing through full-body scanner;
  - Carry out lobbying activities to protect common rights and interests (more efficiency, less costs etc.,)

The policy interactions among stakeholder groups are depicted in Table 1. In this table, columns represent entities that make a policy/decision and rows represent entities affected by that policy/decision. Content in table cells represent which type of decisions/actions one stakeholder can do to others.

Table 1. Interactions between airport security stakeholder groups at different levels

	International Level	European Level	National Level	Regional Level	Operational Level	Travellers
International Level	Regulatory development cooperation	Regulatory, policy advice & contribution	Regulatory, policy advice & contribution	N/A	N/A	N/A[5]
European Level	Regulatory requirement	Regulatory, policy making cooperation	Regulatory, policy advice & contribution	N/A	Regulatory & policy implementation	N/A
National Level	Regulatory requirement	Regulatory requirement	NSP development	N/A	Regulatory & policy implementation Security requirement advice	Policy support or opposition
Regional Level	N/A	N/A	N/A	Collaborate for security measures	Collaborate for security measures	Policy support or opposition
Operational Level	N/A	N/A	N/A	Collaborate for security measures	Balance regulatory requirements, quality of service, revenue & profit	Policy support or opposition Financial support or opposition
Travellers	Requirement regarding safe travel	Requirement regarding safe travel	Requirement regarding safe travel	Requirement regarding safe travel	Requirement regarding safe travel	Balance travel security,

[4] It is reported that drunk passengers are more threats than airport security than the terrorism (http://bemosa.blogspot.no/2012/12/drunk-passengers-more-threat-to-airport.html)

[5] N/A: Not Applicable

	International Level	European Level	National Level	Regional Level	Operational Level	Travellers
					Travel cost and convenience	convenience and cost

3.4. Airport Security Case Study Decision Challenges and Expected Outcomes

The security policy decision-making is a complex and sometimes is a conflicting process. It involves a number of stakeholders, i.e. regulators, policy makers and decision makers, at different levels. It also needs to take into consideration citizens' reactions. As a matter of fact, lower level decision-making processes are more detail but at the same time, they have to comply with those of higher levels. Thus they may have conflicting needs, in addition to challenges of balancing security and cost at regional and local levels.

High-level policy decision challenges of the airport security case study are derived from its high-level security scenarios:

- To select and regulate effective security measures that can face new emerging threats;
- To enforce extensive and "high-quality" training for airport personnel;
- To balance costs of security measures and training among all the airport stakeholders.

Operational-level decision challenges of the airport security case study are derived from the Anadolu operational scenario:

- To implement effective security measures in order to avoid unlawful access to restricted areas in the airport.

4. Critical Infrastructure Security Case Study

The National Grid PLC (NGRID) is a British multinational electricity and gas utility company with business activities in the United Kingdom and North-Eastern United States. In the UK, it owns, manages and operates both electricity and gas transmission networks for the entire country. This includes England, Wales and Northern Ireland. Besides, NGRID owns and operates the distribution of gas in a number of regions of the UK. The company, however, does not manage the distribution of electricity in the UK.

The focus of NGRID's input in the SECONOMICS project is the UK electricity transmission network. While this focus of the research will be in the UK, there may be potential areas of input from the US such as regulatory frameworks and threat landscape of electricity transmission.

In a generic sense, the infrastructure that supports electricity transmission grid consists of the following elements:

- Generators of electricity i.e. coal, gas, nuclear, solar, wind (etc.) power stations;
- Distributors of electricity i.e. those organisations that distribute electricity in a local/regional area;
- Transmission of electricity i.e. high-voltage electrical wiring that connects generators to the distributors;
- The data highway that travels with power cables that provide data about demand, supply, frequency etc.;
- The Supervisory Control and Data Acquisition (SCADA) system that takes the data feed and balances the electrical transmission grid through its links to all generators and distributors.

Since electricity and gas transmission networks form the backbone of the country's energy networks, their security and stable operations play crucial role in the social, business, and political life of the whole country.

WP2 of the SECONOMICS project presents a security case study of NGRID as a critical national infrastructure. This section summarizes security scenarios, threats and impacts of the NGRID case study in deliverables D2.2 and D2.3. We then discuss policy decision-making challenges associated with NGRID case study that the SECONOMICS project needs to address.

4.1. NGRID Security Scenarios, Threats and Security Impacts

This section briefly presents security scenarios, threats and security impacts in NGRID case study presented in deliverables D2.2 and D2.3. A more thorough description can be found in those deliverables.

Security Scenarios

The NGRID case study focuses on the UK electricity transmission network. The case study goal is to investigate security of NGRID's business objects in their current and future states. The business objects under investigation are: (i) interconnectors; (ii) Electricity Management System (EMS) and data links with generators, distributors and interconnectors; (iii) and corporate network and IT infrastructure supporting electricity

transmission. With the plan to roll out smart meters nation-wide in the future, this case study also looks into smart meters as a future business objects.

- Interconnectors – UK currently has electricity connections with France and the Netherlands. In the future, the country will have more connections to Norway and Denmark. The term 'interconnectors' in this context will refer to the corresponding connections in the current and future states;
- Electricity Management System (EMS) and data links with generators, distributors and interconnectors - the EMS manages electricity transmission networks through exchanging information with electricity generators, distributors, and the interconnectors. This includes electricity transmission telemetry and management systems e.g. SCADA systems;
- Corporate network and IT infrastructure supporting electricity transmission - this group can be further divided into subgroups including: (i) business support systems e.g. modelling, demand forecasting, asset management; (ii) and business systems e.g. SAP, Internet etc.;
- Smart meters – apart from recording the energy consumption, smart meters contain switches to turn the supply of electricity on/off and can be remotely controlled by energy suppliers.

Security Threats

A threat is a potential cause of an incident that may result in harms to a system or organization. A threat consists of an asset, a threat agent and an adverse action of that threat agent on the asset (ISO 27005).

In the NGRID security case study, assets are interconnectors, EMS and corporate network and IT infrastructure, and smart meters (in the future states). Threat agents contain threat sources, which are people, or organizations that desire to breach security, and threat actors, which are people or organizations that actually carry the attack. In some cases, a threat source is also a threat actor. A short description of those agents is taken from deliverable D2.3 and is adapted and presented below. More discussions about their capability, motivations and threat levels can be found in D2.3.

NGRID threat sources are:

- Foreign intelligence services/State sponsored group – these are special groups sponsored by nation states with highly skilled agents and very good capability to carry on a potential attack. Their current motivation for attacks in electricity systems is not high however. The current threat level is this type of threat source is substantial while the future expected threat level is critical as their motivations will increase;
- Terrorist group – in contrast with state sponsored groups, terrorist groups often have high motivations to attack a country's infrastructure. However, their skills are not as good as the former one which make possible threats by these groups less serious than those by the former. The current threat level of terrorist group is moderate while the future expected threat level is severe as the capability of terrorist group will increase;
- Organised crime - these are groups motivated by financial gains. Even though there are limited methods to commit fraud or threaten ransom money on a country's electricity transmission network, opportunities exist in the wholesale

electricity market. Organised criminals have capability to deploy multiple computer experts in this area for a significant period of time. The threat level of organised crime in current and future states is expected to be substantial;

- Activists - activists may target NGRID to object NGRID's building of towers or facilities in controversial areas or as a secondary target to the building/commissioning of new power stations. Their motivation is quite low with respect to cyber security space. The current threat level of activists is negligible. However, as their motivations increase, the future expected threat level may rise to 'low' level;
- Hacktivists - this group normally contains lone computer experts working together to target organizations for different purposes. They are also able to command large botnets to perform dedicated denial of service attacks. The current threat level by this group is severe. However, their future threat level will become substantial as they can gain more knowledge and capability;
- Security researchers – this group does not focus on attacking systems similar to that of NGRID at the moment. They however may be a potential threat source in the future as security research in this area gets more attention by academic, institution, and state sponsored groups. The future expected threat level by this groups is moderate;
- Inappropriate regulation - this is also a future threat source based on the NGRID's viewpoint. Incorrectly or inappropriately designed regulatory structures may have a negative impact on the level of security within CNI operators. The expected threat level in the future by inappropriate regulation is moderate.

Threat sources can influence other type threat agents, i.e. threat actors, to carry attacks on their behalf. For each business object, different threat actors may be involved. Typical threat actors in NGRID security scenarios include:

- Employees – this group contains people who actually operate NGRID in different roles. This group can be further divided in subgroups based on threat levels posed by them, i.e. care-less & routine, care-less & business critical, disgruntled, and rogue employees;
- Commercial partners – these are partners involving in NGRID regulatory activities, partners operating the interconnectors, electricity distribution or power generation;
- Service providers – this group contains organizations providing systems and services over those systems for NGRID;
- Physical intruders – these are people who attempt to attack/penetrate systems by gaining physical access to the systems, e.g. breaking into a NGRID site such as a data centre. Also, this threat actor group may attack systems electronically or physically by destroying or sabotaging equipment;
- Malicious attackers – these people attempt to attack NGRID remotely via electronic means or with social engineering techniques;
- Support staff – they are staff working within NGRID sites and are often opportunistic attackers. In particular, they may have legitimate physical access to the most critical NGRID sites but do not have legitimate access to the IT systems.

Security Impacts

NGRID security case study focuses on three current business objects interconnectors, EMS and data links with generators, distributors and interconnectors, and corporate network and IT infrastructure. Disruptions of any of those systems affect to the operation of NGRID and possibly affect the public UK at different levels.

- Interconnectors - they are used to connect a country's electricity grids to those of its neighbours. Different countries across Europe have different levels of reliance on their interconnectors and thus the consequence of security breach involving interconnectors varies. As the UK does not rely too much on the interconnectors to its neighbouring countries, the security impact related to interconnectors is not high for UK. It is in contrast with those for Italy/Switzerland interconnectors because Italy relies a lot on the operation of interconnectors between the country and Switzerland. Thus the security impact of interconnector malfunctioning is very high for Italy;
- EMS and data links with generators, distributors, and interconnectors – for NGRID, the impact of a loss of integrity of data collected by the SCADA systems for managing networks and balancing mechanism is significant while the impact of a loss of availability of the data flowing across the interconnectors is noticeable. However, the impact of loss of confidentiality of data collected by the SCADA systems is in-significant;
- Corporate network and IT infrastructure – in this group, the impact of a loss of confidentiality of the data on the NGRID corporate network is higher than a confidentiality break of live transmission data because a leak of this corporate data outside of the company could result in moderate-significant reputational damage to the company or financial loss due to regulatory fines. Overall, the technical impact of corporate network and IT infrastructure breach is not high in current situations.

4.2. Case Study Validation

The validation in NGRID case study focuses on stakeholders within NGRID and those at national and European levels. As described in deliverable D7.1, the evaluation methods for the output of WP2 by the end of Phase 1 of the project is limited to interviews and discussions with related stakeholder groups.

The work plan of WP2 by the end of Phase 1 is to identify security scenarios & requirements of the NGRID case study. The scenario selection, user requirement development, and result validation of this case study have been developed with contribution and interactions with appropriate stakeholder groups.

More information regarding the involving stakeholders group and validation activities can be found in Section 1.3 "Validation" as well as Appendix 3 of the deliverable D2.3.

4.3. NGRID Stakeholders and Their Decisions

By UK regulation, the only organization in the power delivery chain that an end user has relationship with is his energy supplier. All costs for power generation, transmission and distribution are included in the energy supplier's bill to the end user.

The responsibility of regulating the energy markets in England, Scotland and Wales is independent of government and is given to a quasi-governmental organization, the Office for Gas and Electricity Markets (Ofgem). In the UK, only the energy supplier sector is competitive. Other sectors[6] are monopolistic and the prices charged to consumers for electricity generation, transmission, and distribution are heavily regulated by Ofgem. In addition, Ofgem regulates the amount of profit and prices that energy suppliers can charge consumers.

In electricity transmission, Ofgem's key role is setting price controls on how much NGRID can charge consumers. In order to come up with an agreed number, Ofgem and NGRID need to know the current and future operational costs and investments. However, that requirement may lead to disagreements as it is seen differently from different parties.

The stakeholders in the NGRID case study and their possible policy decisions[7] can be categorized in different levels:

- International level – as NGRID operates both in UK and north-eastern US, it needs to follow regulations by regulators in both countries. Policies made by US regulators, though are not the same, are somehow equivalent to but separated from those made by its European/UK counterparts. For that reason, we only mention possible decisions at European level in the table below.
- European level – stakeholders at this level include regulatory organizations, agencies and working groups. Possible policies/decisions made at this level are:
    - General regulations on strategy, legislation, enforcement, fundamental rights across Europe;
    - General regulations on threat assessment, risk management, cyber security of each nation state as well as at European level;
    - Cooperation for regulatory framework development for this industry across Europe.
- UK level – stakeholders at this level include regulatory organizations, agencies, and Special Interest Groups (SIGs) in UK. Possible policies/decisions made at this level are:
    - Detail regulatory requirements, guidance and advice on security of NGRID, including the rolling out of smart meters;
    - Regulatory requirements regarding pricing and charging models.
- Regional level – in the NGRID case study, there is no regional policy maker as NGRID works directly at the UK national level.
- Operational level at NGRID – possible policies/decisions made at this level are:
    - Operational actions and strategy to manage and mitigate security risks;
    - Decide how to comply with regulatory requirements from higher levels;

[6] Power generation, electricity transmission, electricity distribution
[7] We call a policy decision made by a stakeholder a decision hereafter.

- Future requirements of electrical transmission network.

Table 2 presents policy interactions between NGRID stakeholders at different levels. In this table, columns represent the entities that make policies/decisions and rows represent entities affected by those policies/decisions. At each level, there may be more than one entity.

Table 2 Policy interactions between NGRID stakeholder groups at different levels

	European Level	UK Level	NGRID Level
European Level	N/A[8]	N/A	Regulatory framework & requirement advice
UK Level	Legislative & regulatory requirements	Policy development collaboration	Security investment vs. price models advice
NGRID Level	Regulations regarding threat assessment, risk management, cyber security	Guidance in security, risk management, price vs. charging model	Expense & profit optimization

4.4. NGRID Case Study Decision Challenges and Expected Outcomes

This section presents results that NGRID expects to get out of the SECONOMICS project. From NGRID's perspective, these are security requirements that should be addressed by the project. These requirements form decision challenges that the SECONOMICS framework and tool should be able to solve.

The case study focuses on understanding and assessing information/cyber security regulatory frameworks, which are or could apply to CNI operators. With its framework and tool, the SECONOMICS project is expected to support NGRID in assessing efficacy of two regulatory environments that NGRID operates i.e. in UK and US. Specifically, the project is expected to help NGRID to:

- Decide if current CNI regulations in the UK, and US, adequately and appropriately ensure that NGRID mitigates possible risks in the current states;
- Decide if current CNI regulations in the UK, and US, are flexible and adaptable enough to meet the requirements of NGRID in future states;
- Recommend suitable high-level regulatory structures e.g. risk/principles-based, rule-based, or something else, for NGRID to use in its current and future states.

Though there is no specific requirement from NGRID at the operational level, we believe it would be beneficial if the project could give recommendations so that NGRID can:

- Decide if NGRID UK should comply with all or part of the security guidance suggested by the regulatory bodies as there is a trade-off between providing security (follow all guidance strictly and more) and security investment cost;
- Decide if NGRID US only needs to adhere policies and standards by regulatory bodies or to set higher standards. This is also a security investment cost trade-off.

[8] N/A: Not Applicable

5. Urban Transport Security Case Study

Urban transport is a priority for economic and societal well-being of European citizens living in large cities. According to data from the International Association of Public Transport[9], urban transport ridership has increased steadily over the past 10 years in many EU countries [2]. This trend is expected to continue as cities grow, and challenges like traffic congestion and pollution become more of an issue. However, passengers only use the public transport system if they feel it safe [2]. From transport operators' perspectives, it is essential that they need to invest in security to increase number of passengers and revenue. From a wider societal perspective, increasing urban transport security to promote the use of transport systems will assist the smooth and efficient operation of cities and metro areas.

Regardless of geographic locations and the uniqueness in terms of transport network size and complexity, urban transport systems share common characteristics as far as security is concerned. Such characteristics range from high volume of passengers and the need for quick and easy access to the underground, local trains, buses or trams, to their operations along fixed routes with predetermined stops. All these aspects contribute, on one hand, to make urban transport prone both to daily operational security problems such as disorder, vandalism, and assault, and to exceptional security problems, such as terrorist attacks. On the other hand, these characteristics also contribute to make security controls used in other types of mass transportation, such as passenger and luggage screening, identity checks in airports, impractical for urban public transport [2].

This case study by WP3 of the SECONOMICS project focuses on Barcelona urban public transport. The main public transport operator in Barcelona and Catalonia is Transports Metropolitans de Barcelona (TMB). The metro system of Barcelona is managed by TMB. The company also manages leisure transport services as the funicular railway of Montjüic, Blue tramway and cable car of Montjuïc.

5.1. Urban Transport Security Scenarios, Threats and Impacts

The security purpose of urban transport systems is to guarantee security of transportation services and their passengers. Passenger security has two sides i.e. objective security, which involves threats that affect passengers directly, and the sense of security, which relates to environmental factors or unsocial incidents. The sense of security does not merely relate to the absence of criminal and/or antisocial incidents.

Specific security objectives of urban transport are to minimize costs associated with incidents and at the same time, to minimise number of incidents.

This section summarizes security scenarios and threats in urban transport security scenarios. We also present security impacts of those threats. More information and analysis about urban transport security scenarios, threats and impacts can be found in deliverables D3.2 and D3.3 in WP3 of the project.

[9] www.uitp.org

Security Scenarios and Threats

There are different types of security scenarios and threats that the urban transport has to face with. Within the scope of WP3, the following security scenarios and threats are considered:

- Graffiti and vandalism - graffiti in this context refer to writing, drawing, or spraying on walls or other surfaces of public places without permission. Vandalism relates to the destruction or damage of public structures. Most of these activities are brought about by thrill-seeking and enjoyment of feeling of power and peer recognition without monetary profits;
- Fare evasion by individuals and by collusion – individual fare evasion happens when one tries not to pay a correct fare payment or not to pay tickets at all. Fare evasion by collusion happens when passengers or passengers and the operator's employees collude to avoid paying proper fare. While the former form of fare evasion is based strongly on economic motives e.g., saving money, the latter of fare evasion is more likely to be motivated by social reasons e.g., social bonding.
- Pick-pocketing/theft - pickpocketing and theft are one of the most pervasive types of crime in the Barcelona urban transport. These threats' motivations are solely criminal and economic;
- Tramps – tramps refer to unemployed or homeless people staying in subway stations. The current economic crisis is entailing an increase in their number. As some of them are mentally unstable and disordered and/or aggressive, threats by tramps actually reduce both the perceived and real security of travelling passengers.

Security Impacts

The case study in WP3 focuses on four types of threats in urban transport system as mentioned above. Those threats affect urban transport operators and travelling passengers though their consequences and seriousness are different.

- Vandalism and graffiti – these threats can be categorized as anti-social behaviours because they mostly happen against systems, not against actual travelling passengers. However, those threats reduce passenger perceived security as well as the transport system service quality and reliability. This type of incidents can affect the security of the metro facilities seriously, as graffiti writers often access to train depots or track areas, which can cause service interruptions and sometimes, potential accidents. The economic impact is also high due to expenses to resolve problems caused by those threats;
- Fare evasion – the objective security impact of this type of threat is low because it does not directly affect security of travelling passengers. It however affects passenger perceived security seriously, as it can be considered an antisocial or even a criminal incident according to circumstances. The economic impact of this type of threats to the urban transport operator is enormous. In addition, loss of revenue and profits of operators may influence their decisions to invest on other security measures;
- Pickpocket and theft – the security impact of those threats is very high as these threats directly affect passengers' real and perceived security. The reduction in

passenger perceived security has negative effect on urban transport operators revenue and profit as passengers may choose alternative means of transport;
- Tramps – the security impact of threats by tramps is at medium to high as they can affect passengers' actual and perceived security.

5.2. Case Study Validation

Similar to the security case studies in WP1 and WP2, the main tasks of the urban transport security in WP3 are to identify security scenarios and stakeholders groups in urban transport domain. The security scenarios, requirements, and assessment of current regulatory and decision-making policies of the case study are developed in collaboration with stakeholder groups via interviews and discussions.

As presented in Section 3 "Stakeholders and Engagement Plan" and in Annex 1 "Internal Validation" of the deliverable D3.3, scenario identification and security needs have been developed with interactions from key stakeholders in the urban transport case study, including TMB security division (the urban transport operator) and the transport division of regional police (public authority). High-level requirements were also presented to the SECONOMICS consortium partners during the project's general assembly in Madrid in Nov 2012 for additional comments and validation.

5.3. Urban Transport Security Stakeholders and Their Decisions

Security of urban transport in this case study is less regulated than that of the airport, for which there is a wide range of national-, EU- and international-level legislations involved. In the case of Barcelona urban transport, a regulatory framework governing the TMB operation mainly involves regional and operational (local) level. There are, however, other stakeholders that do not have direct influence at operational level but are also considered for assessment and promotion of innovative operations and technology to enhance public transport security[10]. A detailed list of public transport stakeholders can be found in D3.3.

There are a number of stakeholders involving in the case study and decision-making process of the Barcelona urban transport system. Below main stakeholders and their possible policy decisions are listed:

- Regional level – this includes regional policy forces and rescue services. On this regard, regional Catalonia Government has full competencies regarding railway regulation, as this competence is transferred from the Spanish Central Government. The regional government is also the holder of the infrastructure operated by TMB. Regarding administrative regulations they are hold by the

[10] At international level, only UITP Commission on Security provides studies, assessment and promotes innovative operation and technologies for enhanced Public Transport Security. At European level, DIRECTIVE 2004/49/EC (Railway Safety Directive) applies to railway systems with the exception of Metros, trams and other light rail systems, as they are subject to local or regional safety rules, and supervised by regional authorities. Therefore urban transport is not affected by EU regulations. This is explicitly detailed in Article 2 of the Directive (Scope).

Barcelona Metropolitan Area and the Metropolitan Transport Authority. Possible decisions at this level are:

  - To decide on general regulation of the railway sector in general and underground public transport in particular;
  - To decide on the transportation tariffs;
  - To provide specific security assistance and countermeasures subject to requests and available resources;
  - To provide emergency support subject to request and available resources.

- Operational level – this level includes the TMB and other local transport operators, which TMB has to coordinate on some security issues e.g. Ferrocarrils de la Generalitat de Catalunya, RENFE Rodalies, TRAM Baix & TRAM Besòs. Decisions at this level include:
  - To provide proper security measures based on general guidelines;
  - To provide acceptable quality of service;
  - To balance security and quality requirements with expenses.
- Citizens, passengers and users in general can also decide:
  - To take alternative means of transport;
  - To oppose to specific regulations or measures.

The policy makers, public authorities, organizations and institutions make decisions according to public interest at three different levels: the strategic level to set the objectives and goals to achieve; the tactical level, in which services and security measures are set and, finally, the operational level when services and security measures are implemented [2].

The policy interactions among stakeholder groups are depicted in Table 3. In this table, columns represent entities that make policies/decisions while rows represent entities affected by those policies/decisions. Cells in the table represent which type of actions/decisions stakeholders can do to the others.

Table 3 Interactions between urban transport stakeholder groups at different levels

	Regional Level	Operational Level	Passengers
Regional Level	Collaborate to decide regulations of the urban transport in particular and railway section in general	Comply with guidelines to provide security measures	Pressure on security and quality of service policies
Operational Level	Regulate security practice via regulation. Collaborate to protect security & share costs[11]	Balance security requirements and expenses, maximize security-cost function	Pressure on security measures, fare, and quality of service
Passengers	Provide actual & perceived security	Provide actual & perceived security Provide service quality & good fare	Choose to take alternative means of transport

[11] Regional police forces and rescue services

5.4. Urban Transport Security Decision Challenges and Expected Outcomes

In order to increase security of Europe's transport systems, it is necessary: (i) to develop and accept a common socio-economic methodology for decision support in security across EU countries; (ii) to develop adequate standards and procedures for harmonised implementations of solutions and services consistent with the defined framework; and (iii) to support the implementation of security measures taking efficiency, business and societal impact into account.

High-level policy decision challenges of the urban transport system case study include:

- To take into consideration various security concerns from all stakeholders and identify possible threats;
- To carry on risk assessment taking into consideration the probability of occurrence and the impact;
- To provide good practice guidance on how to implement proper security policy that balances available cost and threats;
- To provide persuasive reasoning and communicate with involving stakeholders[12];
- Take into consideration social and sociological implications of security measures, as security perception is as important as objective security.

Operational policy decision challenges of the urban transport system include:

- To balance between security, cost and service quality[13].

[12] Though threats can be common across operators, even across countries, required policies must take into account cultural differences, and must be flexible enough to allow local adaptation.

[13] An example is a 24h metro service at weekends. Though it provides excellent service from passengers' viewpoints, it is not very profitable and at the same time it can introduce more security incidents.

6. Cross-Domain Decision Challenges

A policy decision-making process may involve three groups of stakeholders: (i) regulators and policy makers; (ii) CNI operators; (iii) and public citizens. Stakeholders in group (i) can be further divided into different levels of the policy-making process that they involve. They can be at international or supra-national level, European, national or regional level. Stakeholders in group (ii) are often referred to operational or local decision makers in this report.

The case studies in WP1, WP2, and WP3 discuss specific security requirements and decision-making challenges in different critical infrastructure domains. These domains have both common and distinct policy decision-making needs.

This section generalizes common decision challenges across those domains. Some common decision challenges apply for all three domains while others may only apply for two of them. In this section, we choose to address cross-domain policy decision-making needs from the top-down approach based on levels of the policy decision-making process. We only discuss possible common policy decisions between domains.

- Supra-national or international level - the airport security case study involves international regulators (e.g. ICAO). The NGRID case study involves non-European regulators as it also operates in north-eastern US. The NGRID needs to comply with regulations from both UK and US. However, there are no common decision making challenges at international level between the airport and NGRID case studies.
- European level - both the airport security and NGRID case studies involve policy makers at European level. The common decision making needs include:
    - Decision on the rights of citizens in relation with the use of CNI;
    - Decision on the general security strategy and legislation for the industry across Europe;
    - Decision if current regulations meet security requirements in that domain for both current and future threats.
- National level - both the airport security and NGRID case studies involve policy makers at national level. Policy makers at this level need to decide on specific security requirements for their countries based on general guidance from higher-level regulators. The common security decision-making challenges for these two case studies include:
    - Decision if current security regulations at national level meet security requirements in that domain;
    - Decision on security clearance requirements for personnel working at the CNI infrastructures.
- Regional level: both the airport security and urban transport system case studies involve policy makers at regional level[14]. As the regional authorities also participate in guaranteeing security in both case studies, common decisions made by regional decision makers are:

[14] In NGRID case study, there is no regional policy maker as NGRID works directly with the UK regulators.

  - Decision on types of specific operations the regional authorities should involve, together with the CNI operators, to protect security;
  - Decision on how regional authorities interact with the CNI operators should security incidents happen.
- Operational (local) level - all three case studies involve decision making at operational levels. Though the case studies focus on different domains, there are common decisions they need to consider:
  - Decision whether they should implement specific security measures – as many security requirements are guidance of generic specifications, it is up to the operational decision makers to implement specific security measures to address the requirements;
  - Decision on how to implement specific security measure as different levels of implementation result in different security-cost trade-offs. They also affect citizens' sense of security and convenience.

The case studies of airport and urban transport also involve citizens as end users. Though they cannot make any regulatory policies, citizens can make their own decisions (financially or politically) to support or oppose specific policies. Thus the decisions from citizens will also be taken into consideration during the SECONOMICS framework development. Cross-domain decisions made by the citizens are:

- Choose to support or oppose to CNI operators by using alternative services or by not using the service at all. This type of actions affects the operators economically and thus, will affect their decisions;
- Choose to support or oppose to higher-level policy makers with social or political campaigns.

7. Summary of Impacts on SECONOMICS Security Missions

As mentioned in Section 2, the project sits within the FP7 security research theme with four security missions and three cross cutting missions. The Anadolu airport security case study addresses all security missions while the other two case studies addresses security missions 1, 2, and 4. The case studies also address cross cutting missions 2 and partially address the cross cutting mission 1. Cross cutting mission 3 is a result of the project collaboration.

This section briefly presents how three case studies address security and cross cutting missions in the SECONOMICS project.

- Security mission 1 - Security of citizens
  - With proper airport security policy and measures, the travelling public are protected from accidental and intentional threats, including crime and terrorist attacks;
  - The case study of NGRID contributes to the protection of the GRID as a national infrastructure from security incidents. This will prevent electric surges and power outage from happening and thus to protect citizen equipment and their daily lives. Power outages, depending on when and where they happen and how long they last may have different effects on citizens' lives;
  - Similarly, as urban transport systems play a crucial role in transporting citizen in European cities and metropolitan areas, they attract a large number of passengers daily. Security and safety of urban transport systems directly affect security and safety of citizens. This case study in security of Barcelona urban transport system will contribute directly to security of citizens in the city.
- Security mission 2 – Security of infrastructures and utilities
  - As airport operations directly affect the economic, political, and social activities of a specific region and possibly a country, an airport is a critical infrastructure and utility of that area. Guaranteeing safe, continuous and efficient operations of the airport is crucial for the development and stability of the region;
  - NGRID provides electricity and power not only for citizens' daily lives but also for business and other social and political activities. NGRID is a critical infrastructure and utility serving for a normal operation of the society. WP2 investigates and contributes to the security development of NGRID and thus addresses the security of infrastructures and utility requirements as targeted by the SECONOMICS project;
  - Urban transport systems are critical infrastructures of modern societies and their efficient and continuous operation are crucial, both for business and for security and safety of citizens. The urban transport case study contributes directly to the protection of urban transport systems as critical infrastructures and utilities.
- Security mission 3 - Intelligent surveillance and border security
  - Since an airport is often an entry/departure point of a country, airport security directly and greatly affects a country border security. A good

airport security program will contribute the protection of a country borders in addition to the protection of citizen flow crossing those borders.

- Security mission 4 - Restoring security and safety in case of crisis
    - The Barcelonan urban transport case study in the project focuses on methods and procedures to restore security and safety of a metro system in case of crisis incidents. Results from this case study will be used as inputs to the other two case studies. Upon the completion of the SECONOMICS project, we will develop a framework that is able to tackle the problem of restoring security and safety of the airport and critical infrastructure operations in case of crisis.
- Cross cutting mission 1 - Security systems integration, interconnectivity and interoperability
    - The case study about airport security in WP1, together with the case studies in WP2 and WP3, will contribute to the development of different components of the SECONOMICS framework. As the framework provides cross-mission policy decision support tool, its components are interoperable. The framework can also integrate with existing policy tools.
- Cross cutting mission 2 - Security and society
    - Airports are major border control entities as well as economic driving engines for particular regions/countries. Thus safe and efficient operations of airports greatly and directly affect societal security and economic stability. Results from the airport case study contribute to the achievement of these goals;
    - The UK National Grid case study focuses on addressing the possible security problems associated with NGRID and by doing so, it will help to protect the NGRID as a CNI operator in particular and the UK and European modern society in general from security threats that can harm the UK's society;
    - Operations of urban transport system are critical to daily personal, political and business activities and normal operation of the society. Protecting urban transport systems contribute to security of the society as a whole. This case study, together with the other two will contribute to development of the SECONOMICS framework that supports cross-domain multi-level policy decision. The output of SECONOMICS will then be generalized and applied to other critical domains to increase security in society overall.
- Cross cutting mission 3 – Security research coordination and structuring – this mission is addressed by the collaboration between all partners of the research consortium.

8. Conclusion

This deliverable consolidates user requirements from three case study work packages WP1, WP2, and WP3 of the SECONOMICS project. We briefly discuss security scenarios, threats and impacts to provide overall security pictures in each case study. A list of stakeholders and their possible decisions in each case study is discussed and presented. These stakeholders and decision requirements will then be used as inputs for the SECONOMICS technical work packages. At the end of each case study section, we present requirements from that case study which the project need to address. Depending on the operation nature of each case study partner, the requirements vary and apply at different levels, from international regulatory level to regional decision-making level to operational level. The report also generalizes cross-mission decision challenges, which are high-level requirements commonly applied to more than one case study.

The identified key requirements of each case study work package, together with common requirements among them, will then be used as input to the technical research work packages WP4, WP5, and WP6.

REFERENCES

[1] D1.3 Airport Requirements Final version, FP7 – SECONOMICS Report, V. Meduri, F. Quintavalli, A. Tedeschi (DBL), B. Açikel, N. Ergün, U. Turhan(AU), M. De Gramatica, Woohyun Shim (UNITN), D. Rios Insua (URJC), J. Williams (ABDN).
[2] D3.3 Urban Transport Requirements Final version, FP7 – SECONOMICS Report, R. Munné (Atos), M. Pellot (TMB), Ricardo Ortega (TMB), Daniel Villegas (TMB).