SECONOMICS

D7.3 – Aggregate SECONOMICS Framework

A. Couce Vieira, S. Randall (SNOK), J. Williams (UDUR), P. Rakusanova Guasti (ISASCR), J. Cano (URJC), F. Massacci, W.Shim (UNITN)

Pending of approval from the Research Executive Agency - EC

Document Number	D7.3
Document Title	Aggregate SECONOMICS Framework
Version	1.0
Status	final
Work Package	WP 7
Deliverable Type	Report
Contractual Date of Delivery	30.04.2014
Actual Date of Delivery	09.05.2014
Responsible Unit	SNOK
Contributors	SNOK, DURHAM, ISASCR, URJC, ABDN, UNITN, DBL
Keyword List	Critical infrastructure security, security policy models, security risk models, security and society models
Dissemination level	PU

SEVENTH FRAMEWORK PROGRAMME

Security Economics: Socio economics meets security

SECONOMICS Consortium

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

1	UNIVERSITÀ DEGLI STUDI DI TRENTO	Università Degli Studi di Trento (UNITN) 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	1495 UNIVERSITY OF ABERDEEN	THE UNIVERSITY COURT OF THE UNIVERSITY OF ABERDEEN, a Scottish charity (No. SC013683) King's College Regent Walk, AB24 3FX, Aberdeen, United Kingdom http://www.abdn.ac.uk/	Contact: Dr Matthew Collinson matthew.collinson@abdn.ac.uk
6	TMB Transports Metropolitans de Barcelona	FERROCARRIL METROPOLITA DE BARCELONA SA, Carrer 60 Zona Franca, 21-23, 08040, Barcelona, Spain http://www.tmb.cat/ca/home	Contact: Michael Pellot mpellot@tmb.cat
7	AtoS	ATOS ORIGIN SOCIEDAD ANONIMA ESPANOLA, Calle Albarracin, 25, 28037, Madrid, Spain http://es.atos.net/es-es/	Contact: Alicia Garcia Medina alicia.garcia@atos.net
8	SECURENOK	SECURE-NOK AS, Professor Olav Hanssensvei, 7A, 4021, Stavanger , Norway Postadress: P.O. Box 8034, 4068, Stavanger, Norway http://www.securenok.com/	Contact: Siv Houmb sivhoumb@securenok.com
9	SOÚ Institute of Sociology AS CR	INSTITUTE OF SOCIOLOGY OF THE ACADEMY OF SCIENCES OF THE CZECH REPUBLIC PUBLIC RESEARCH INSTITUTION, Jilska 1, 11000, Praha 1, Czech Republic http://www.soc.cas.cz/	Contact: Dr Zdenka Mansfeldová zdenka.mansfeldova@soc.cas.cz
10	nationalgrid THE POWER OF ACTION	NATIONAL GRID ELECTRICITY TRANSMISSION PLC, The Strand, 1-3, WC2N 5EH, London, United Kingdom	Contact: Dr 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
12	Durham University	The Palatine Centre, Stockton Road, Durham, DH1 3LE, UK	Contact: Prof. Julian Williams julian.williams@durham.ac.uk

Document change record

Version	Date	Status	Author (Unit)	Description
0.1	31/05/2013	Draft	S.T. Nguyen (SNOK)	Draft
0.2	29/08/2013	Draft	S. Cadzow (SNOK)	Update of Draft
0.3	15/11/2013	Draft	F. Massacci (UNITN), J. Williams (UNIABDN), S. Cadzow (SNOK)	Update of Table of Content Update of Draft with Ontology structure
0.4	27/11/2013	Draft	S. Cadzow (SNOK)	Removal of Ontology structure
0.5	23/01/2014	Draft	S. Cadzow(SNOK)	Management level overview of project
0.6	05/02/2014	Draft	S. Cadzow(SNOK) A. Couce Vieira (SNOK)	Proposing deliverable content structure and examples
0.7	03/03/2014	Draft	S. Cadzow(SNOK) A. Couce Vieira (SNOK)	First complete draft for project review
0.8	07/04/2014	Draft	A. Couce Vieira (SNOK) J. Williams (DURHAM) F. Massacci (UNITN) P. Rakusanova Guasti (ISASCR) J. Cano (URJC)	Second proposal for including changes agreed in the project review
1.0	02/05/2014	Final	A. Couce Vieira (SNOK) S. Randall (SNOK) J. Williams (DURHAM) P. Rakusanova (ISASCR) J. Cano (URJC) F. Massacci (UNITN) E. Chiarani (UNITN) W. Shim (UNITN)	Final version after revision and quality check, and with additional contributions

INDEX

1. Introduction

This current document presents a summary of the **Aggregate SECONOMICS Framework.** The SECONOMICS framework provides a toolkit to support those responsible for choosing the optimal level of investment in security measures and strategies for a variety of different types of critical security domains taking into account the socioeconomic context and implications.

The remainder of the document is structured as follows:

Overview of the SECONOMICS Framework	Description of the SECONOMICS Framework and how it provides security policy, risk and societal models and insights to both operational and public security policy-making.
Security Missions and the SECONOMICS Framework	Explanation on how the SECONOMICS address EU's FP7 Security Missions.
Framework Structure	Categorization of the models and tools of the SECONOMICS framework in regard to their policy level.
Validation Scenarios	Description of the validation carried out to ensure that the research activities meet the case studies requirements.
Toolkit Implementation	Description of the SECONOMICS toolkit implementation.
On-going work	Description of the on-going work of the project.
Summary	Summary of the SECONOMICS Framework.

1.1 Overview of the SECONOMICS Project

SECONOMICS is a European collaborative research project on the socioeconomics of security in respect to critical infrastructure, urban transport and air transport. The aim of the project is to enable a broad approach to modelling security to assist decision-makers at both public and operational policy levels. SECONOMICS accomplishes this in two ways. First, by assessing the current and emerging threats as well as the optimal policy measures to mitigate them. Second, by providing a policy framework and toolkit to assist in formulating an appropriate response taking into account the key socioeconomic issues involved.

This support will help public and operational policy makers responsible for the security of the research areas in question to invest and make operational decisions with a more complete picture of the implications and potential impacts as they vary their security-choices. The well-established scientific basis of the research activities in this project, as well as the associated validation process is the major advance of the SECONOMICS Framework.

SECONOMICS is driven by three case studies in key critical security domains (airport, energy distribution and urban transport), and by three interrelated research activities (security policy models, security risk models, and security and society models). The security domains represent a cross section of critical infrastructure (CI) security, the study of which provide important evidence for a much broader set of security domains (such as the oil and gas industry, gas distribution, water distribution and treatment and information networks). The project has identified concrete security issues in the case studies that served as input for the later R&D activities. These then characterised threats and developed models, techniques and methods based on rigorous and well-established research from economics, operations research, security and social sciences. The practical suitability of these models has been validated within the case studies and this is an on-going process.

2. Overview of the SECONOMICS Framework

The SECONOMICS Framework consolidates the project research activities and synergies by focussing on the provision of policy outcomes based on a thorough and comprehensive approach to CI security. SECONOMICS develops both the research and application domains of security. It extends the research domain to include a complete assessment of social aspects with more formal models and systems for policy-making and risk assessment. The application domain of CI security is also enhanced by the provision of a set of complete and implementable CI security policies derived from such thorough research.

A **Policy** is a principle of action adopted by an organization. It guides decisions, it is implemented as a procedure and it aims at achieve a specific outcome. SECONOMICS identified two major categories of CI security policy:

- **Operational policy**
    - Adopted by any organization - business, non-profit or governmental – to:
        1. apply or align with a public policy on CI security, or
        2. directly address a specific security problem within the operational context of the infrastructure,
    - Operational policies may be in line with business governance frameworks and should comply with law and regulations (i.e., public policy). Their outcomes are expected to affect the specific infrastructure,
- **Public policy**
    - Adopted by national, regional, European or international organizations,
    - Established as laws or directives by government agencies or legislators,
    - Outcome is expected to affect the national or regional level as well as the societal.

The SECONOMICS framework addresses both public policies (taking place in **strategic scenarios**) and operational policies (**operational scenarios**) related to the security of CI. SECONOMICS identifies a set of public, operational and societal policy decision-making processes. The goal of public policy making at the European level is coordination and information sharing. The enactment of mandated security provisions (such as investment, audit and security control compliance) for CI resides mainly at the national level and, as such, has diverse delivery mechanisms across EU member states.

Operational decision-making by the CI operator is normally based on recommendations or requirements from an appropriate public body. In many cases, such as in the airport security domain (Case-Study 3), the degree of operational discretion is extremely limited. In the case of bulk-electricity transmission (Case-Study 2) the CI operator has full discretion in security policy although decision are taken in very close cooperation with the relevant public bodies. The situation in the regional transport domain (Case-Study 3) lies somewhere in between these two boundaries.

A final important decision-making level to be considered is the societal one. Although ordinary citizens cannot implement any regulation or policy directly, they are able to make their own economic and political decisions to support or oppose specific policies.

SECONOMICS has taken steps to identify the picture of CI security within which its research activities take place and the space of decisions where security policies have to be implemented. The project research pivots on three key topics which, if enhanced, will significantly improve CI security as a whole. These topics are:

- **Security policy models** based on Economic and system models,
- **Security risk models**, and
- **Security and society models**.

SECONOMICS describes a systematic approach to public policy-making that models the interactions and implications of such policy including economic and societal aspects. The project also provides a means of improving operational security through the enhancement of risk assessment which is one of the key security activities, to include motivational aspects and a more rigorous approach to risk quantification. Finally, the project not only takes into account the technical aspects of security research but also sets citizens and users as key and active parts of security assessment, policy-making and measurement implementation.

SECONOMICS enhances security research by assessing more thoroughly the stakeholders and agents involved and by looking closely at the strong and interactive relationships that exist between them. CI security public policy-makers respond to citizens but also have their own mandate to govern on behalf of the citizens.

Public policies should be aligned with the policies of CI operators and take into account both societal/government and business goals and missions.

Operational CI security should consider the continuous interaction with citizens as users, consumers or just stakeholders affected by their activities. All of these exist in the presence of a fourth actor, the threatening agent intent on supporting or perpetrating attacks against citizens, governments, organizations or infrastructure. SECONOMICS shows how these agents and their interactions are significantly affected by risk and security perceptions. More importantly, it shows how necessary it is for policy-makers to consider and deal with these risk and security perceptions.

Closer integration between CI policy-making, risk management and the management of the social mission and accountability is required in order to avoid partial and, sometimes, contradictory solutions. SECONOMICS research based on its case studies underpins this integration by providing new insights and policy recommendations in the activities necessary for achieving good and complete security results.

CI security policy-makers should ensure that regulations and policies are both implementable and effective. This is achieved through a systematic and scientific approach to the many challenges that compound the security problems faced. SECONOMICS' comprehensive security policy models [D6.1, and D6.2] provides scientific, validated but pragmatic support for such decision-making. This will not only assist in security public policy making but also provide a consolidated information resource to support interaction with other departments, agencies or policy-makers outside security. Furthermore, the resultant public policies will to provide mature and more focused requirements for the security governance of CI operators and, ultimately, the implementation of optimized security measures.

Well-established economic and system models form the basis of this support. SECONOMICS parameterizes these models using a more granular approach to the modelling problem. Specifically, they consider the public economics and governance foundations of CI security as key processes by which the security of citizens is provided. Social contracts with citizens for the provision of an environment which is both safe and secure are considered. Although operational security deals with and interacts with societal aspects, it is through public policy that operational measures and citizens interactions with security are mediated.

SECONOMICS' combination of both security policy and social preferences provides a powerful tool for informing policy-makers and citizens and for connecting citizens' security requirements and considerations with the operational security measures implementation.

Conceptualizing Regulation

In reality there are a number of issues that need to be considered in the formulation of CI security regulations:

- The benefits of regulation based on rules – typical of the US context – versus those based on principles – typical of Europe - [D6.2:1],
- the provision of a theoretical framework for public policy intervention in information security, and
- the dichotomy between audit-based systems and risk-based systems [D6.2:2].

This evaluation characterizes the optimal regulatory approaches or structures for security CIs such as airports [D1.4] or electrical grids [D2.4] to reduce risk taking into account the behaviour of the infrastructure operators, threat agents, and public. Both economic and social insights to behaviour (such as game theory and the risk and security perception) serve as a basis of this characterization.

Effective operational security also relies on the quality of its risk assessment since this affects all of the other technical, management and governance security activities and measures. However, a traditional risk-based approach to security is not enough. The different nature of CI security and the consequences of uncertainty require the less rigid and more powerful analysis of the SECONOMICS risk model which captures the motivations and expectations of the actors involved (including the threat agents) and which enhances the quantification of risk and modelling of the more complex interactions in the real world. Since an enhanced risk assessment improves CI operator security, it will also improve CI public security decision-making by providing clear insights for public policy-makers on what is or could be going on at the operational level.

SECONOMICS provides a complete methodology for CI security risk assessment using Adversarial Risk Analysis (ARA). Traditional risks analysis focuses on categorizing risks based on their likelihood and impact, often by means of very basic tools such as risk matrices. ARA [D5.1] enhances the assessment of risk scenarios through

- the incorporation of both the attacker and defender decisions,
- a more formal and consistent approach to modelling uncertainties such as the likelihood of an occurrence of the attack and outcomes of the attack, and
- the projected motivation of the agents (through the decision that makes them expect a better result due all the uncertainties they face).

The scientific basis of ARA modelling [D5.1:1-2] is a mathematical and computational approach while the graphical representation of ARA models [D5.2:2-3] is an effective mechanism for understanding the problem despite the underlying rigour and complexity of the framework. Within the SECONOMICS project ARA has been applied to the modelling of security risk scenarios such as unlawful access to an ATC tower in an airport [D5.2:2] and fare evasion and pickpocketing in metro stations [D5.2:3]. It provides a successful validation of the models as well as useful recommendations and insights to the operators of such critical infrastructures.

The inclusion of social aspects completes any analysis of CI security by going beyond governance, risk and compliance and considering feedback from society as both citizens and users of the infrastructure. SECONOMICS leads a change in approach to CI security from having people and social aspects as something fixed and based on assumptions which are sometimes doubtful, to a new paradigm where social aspects have a key and variable role in CI security by considering:

- how they influence other aspects of security such as risk and public policy
- how they are influenced by other aspects of ,
- the impact of technical implementation or security communication at both public and operator level.

Being based on data from several countries, SECONOMICS, has been able to assess the perceptions and attitudes of citizens towards risk, security measures and the trade-offs involved (such as the contradiction between freedom or privacy and security) [D4.2]. These factors vary between countries and time as changes in public knowledge of these threats and measures increases. SECONOMICS found that punitive and preventive measures have the potential to both increase and decrease perceived security. The key issues for security policy are

- clear and unambiguous communication with stakeholders and citizens in regard to security and risk, and
- the debates and justifications of security and risk and how the media communicates these to citizens.

SECONOMICS evaluated both communication channels and communication patterns (supported by direct observations, media analysis, interviews, and statistical data), and found that new ways of communicating policy are required. The most Important factors identified [D4.3, D4.4] are that:

- authorities and operators should communicate security measure to users, paying attention to users perception and acceptance as well as ensuring a thorough analysis of users complaints [D3.4], and
- the impact of media debate and salience in putting threats [D4.3, D4.4] such as CCTV [D3.4] and Stuxnet [D2.4], into the everyday or direct usage of citizens). Public media is devoting more and more coverage of security trade-offs between cost, privacy, health and freedom. However, this coverage varies with the cultural, security and media context. Traditional media tends to underestimate security experts and civil rights groups although the involvement of citizens in the security debate is weak. SECONOMICS proposes that European institutions should lead a movement to increase the visibility of the security debate, involve more parties, provide more communications channels and, more importantly, establish EU-wide independent, critical, and accessible news sources.

At the same time as needing to know the technology or processes to be secured, it is also necessary to know the behaviour of people and their attributes when specifying security in general and CI security in particular. The security and social models feed the security risk models by providing the actual aspects to consider when implementing security measures. In addition, there are legal, policy and business requirements to be complied with and implemented as security measures and there are social requirements projected by people more directly or indirectly through public policy.

Part of the work across SECONOMICS is to build a toolkit that integrates the models that operate at the public-policy and operational-policy levels. SECONOMICS is addressing that by:

1. building a software toolkit with the core models to support policy-decision making to find the optimal security resource allocation, and
2. developing a method to generate infographics and communicate security complexities in a more useful way.

SECONOMICS has achieved consistent results in the validation of its models in terms of the suitability for the domain and technical usability. SECONOMICS models were broadly well accepted by the security specialist and policy makers at CI, who find the framework relevant and useful for their activities. A series of structured validation processes have demonstrated that SECONOMICS approach provides a broader assessment of CI security with an approach which more structured and logical than traditional approaches [D1.4, D2.4 and D3.4]. An important aspect of this approach is the provision of a comprehensive strategic analysis of security problems from the viewpoint of public coordination through to citizens' perceptions of security. The models provide an improvement in the technical capabilities of security modelling and assessment and are comprehensible enough for security specialists and policy makers at CI to use although the scientific and novelty nature of the models make some guidelines and consultancy necessary. Section 3 provides a detailed summary of how the research methodologies:

- map across security missions,
- catalogue the various models developed for SECONOMICS, and
- map the sections for the relevant deliverables.

Section 4 provides a summary of the Aggregate-Framework and a comprehensive roadmap for this framework. Section 5 summarises the validation process and provides a project-wide map of deliverables.

3. Security Missions and the SECONOMICS Framework

SECONOMICS addresses, as other EU projects, the EU'S FP7 Security Missions that provide principles to drive security at the European level. The following table describes the EU's FP7 Missions (security missions – SM – and cross-cutting missions - CM -) and how the SECONOMICS Framework provides models that fulfil such missions:

EU'S FP7 SECURITY MISSION	SECONOMICS FRAMEWORK	
SM1. SECURITY OF CITIZENS: Concerns 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.	Economic model applied to the optimization of airport security regulation provides an improvement of the process of regulatory decision-making [D1.4]. Media analysis applied in the case studies provides information about the perception and acceptance of security measures such as CCTV [D3.4] and risks such as Stuxnet [D2.4]. The social model applied to the airport security case [D3.4] shows that customer acceptance is higher for established technical security measures such as CCTV than for human measures or new technical measures such as reversible automatic doors.	Security policy models for: • optimizing security regulation structures [D6.1, D6.2, • optimizing social outcomes [D6.1], and • providing support for the selection of strategic measures for protecting citizens and infrastructures against crime and terrorism taking into account public opinion, attacker behaviour, and how the measures could be implemented by CI operators [D6.2:3]. The security risk model uses Adversarial Risk Analysis [D5.1, D5.2] to provide: • a way to optimize security resource allocation taking into account intelligent adversaries and complex scenarios, and • optimal operational strategies to the security policy models at public policy level. Security and society models provide: • support on key factors for improving citizens' and infrastructure [D4.2], • communication channels and communication patters in security and risk [D4.3], and • discourses and justifications of security and risk through media analysis [D4.4]. All of these provide social preferences [D4.2, D4.3] and behavioural [D4.4] inputs for enabling the integration of public opinion into security policy models. Security and society models also provide the
SM2. SECURITY OF INFRASTRUCTURES AND UTILITIES: Concerns the protection of critical infrastructure and utilities in the European society, including all computerized support. Infrastructures are critical in a modern society and their efficient and continuous operations are crucial, both for business and for security and safety of citizens. The important goals are to identify, prevent, protect and react to security threats happened to these infrastructures.	The security risk model applied to the airport's cyber security threat scenario provides useful information related to the securing of critical IT infrastructures through the analysis of critical vulnerabilities and controls, investment insights, and hacker behaviour [D1.4]. Economic and system models assess which type of regulatory structure is best to incentivize infrastructure operators to improve cyber security s [D2.4].	

		behavioural characteristics [D4.2] required for the security risk models.
SM3. INTELLIGENT SURVEILLANCE AND BORDER SECURITY: Concerns 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.	SECONOMICS does not directly address border security. However, the methods of the SECONOMICS framework can be used to set up a tailored and adaptive resource allocation strategy and both the security risk [D5.1, D5.2] and security and society models [D4.2, D4.3, D4.4] provide insights into the selection of effective measures considering their acceptance by customers or users.	
SM4. RESTORING SECURITY AND SAFETY IN CASE OF CRISIS: 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. The emphasis is on issues such as general organisational and operational preparedness to cope with security incidents, 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.	SECONOMICS addresses this mission indirectly as it applies to specific micro-scale incidents rather than public and operational level security. However, the models use shock response methodologies to calibrate the overall security models. Thus, much of the modelling framework covers incident response implicitly. For instance, the ARA models [D5.2] used for validation in D1.4 include incident response within their modelling framework. The policy models in D6.2 specifically address changes in attacker behaviour and explicitly model incidents such as changes in the efficacy of attackers generating threats to bulk electricity transmission (see also D8.2 and D8.3 for visualisation).	
CCM1. SECURITY SYSTEMS INTEGRATION, INTERCONNECTIVITY AND INTEROPERABILITY: Addresses the integration, interconnectivity and interoperability across various security systems.	The SECONOMICS framework addresses indirectly this mission as it asses the physical and operational consequences of cyber attacks in networked systems [D1.4, D2.4] which are key in the integration of CI security systems. Additionally, the modelling techniques are tailored for the analysis of national and supranational CI.	
CCM2. SECURITY AND SOCIETY: 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 SECONOMICS framework is derived from research and validation tailored to Europe's security needs and context. In addition, most of the security policy models [D6.1, D6.2] are directly applicable to decisions made at European level, particularly to public policy and regulatory structures.	
CCM3. 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.	

4. Framework Structure

	PUBLIC SECURITY POLICY	OPERATIONAL SECURITY POLICY
SECURITY POLICY	• Assessment of public regulatory and	• Guidance on how to model [D6.1:2], test

<table>
<tr><td>MODELS</td><td>policy regimes, including an explanation of the varying efficacy of principle-based regulation as opposed to rule-based regulation. [D6.1:1, D6.2:1],
• A framework for public policy in information security, and
• The dichotomy between audit-based approaches and risk-based approaches [D6.2:2].
• Introduction to achieving optimal social policy outcomes using a public policy model [D6.1:9] based on social utility functions, with an illustration on how it can be applied to securing industrial control systems in bulk-energy transmission [D6.1:10].
• Supporting models of principal-agent, incentives and externalities for security policy [D6.1:1], cost-benefit analysis and inter-temporal decision-making [D6.1:8].</td><td>[D6.1:3] and implement [D6.1:4-5], even as a software tool [D6.1:6], consistent and applicable organisational security architecture models for policy implementation, with an application in airport security [D6.1:7] that demonstrates the implementation suitability.
• Summary of how the public regulatory and policy regimes can be implemented in an organisation [D6.2:3] to enable the operative execution of the public policies.</td></tr>
<tr><td>SECURITY RISK MODELS</td><td>• Provision of optimal resource allocation strategies at operative level [D5.2] as an input for public policy models, enabling policy-makers determine which are the most appropriate measures to implement in their security policies.</td><td>• Introduction to Adversarial Risk Analysis (ARA) as an evolution of standard risk analysis for dealing with strategic adversaries [D5.1:2], including its application in realistic scenarios such as unlawful access to an airport ATC tower [D5.2:2] and fare evasion and pickpocketing in public transport [D5.2:3].</td></tr>
<tr><td rowspan="2">SECURITY AND SOCIETY MODELS</td><td>• Assessment of risk perception and attitude of citizens toward risk, security and the trade-offs involved [D4.2].
• Provision of social preference [D4.2, D4.3] and behavioural [D4.4] inputs tailored to public policy models, enabling policy-makers estimate the impact on public opinion of their security policies.</td><td>• Assessment of communication channels and patterns in security and risk, and provision of highlights to new and effective approaches to communication patterns and channels [D4.3].
• Provision of behavioural characteristics [D4.2] as inputs to security risk models, enabling risk-modellers determine the preferences and perceptions of social agents and, thus, estimate their behaviour and motivation.</td></tr>
<tr><td colspan="2">• Evaluation of discourses and the justification of security and risk, through media analysis of public attitudes toward security issues of airport, electrical grid, and public transport infrastructures [D4.4].
Explanation of the important difference between perceived and actual security and the varying effect of punitive and preventive security measures on perceived security [D4.3].</td></tr>
</table>

5. Validation Scenarios

The research activities that are the basis of the SECONOMICS Framework were validated by a complete process that proves that the Framework complies with user requirements and that its functionality is correct. This validation process [D7.1] was driven by three high-level objectives:

- user acceptability,
- domain suitability, and
- technical usability

These were also refined into more measurable validation criteria, indicators and metrics. Various methods were used to validate, integrate and apply the models, methods and tools of SECONOMICS to the case studies. The first step of validation was identifying the stakeholder's operational needs [D7.2] after which the models were validated [D1.4, D2.4, D3.4] according to the specified validation objectives.

CI	LEVEL	SCENARIO	MODEL	METHOD
AIRPORT	Strategic	Effective airport security regulations [D1.4:2.1] to incentivize airports to invest in security measures at a social optimal level.	Economic models for optimization of airport security regulatory structure to reduce risk and maximize social optimum [D1.4:2.3, D6.1, D6.2].	• Scenario-based simulation, • focus group, • model customization, and • envision of the tool [D1.4:3]
	Operational	A hacktivist group attempts to carry out a cyber-attack that could compromise baggage checking and therefore delay flights.	Adversarial Risk Analysis model [D1.4:2.3, D5.1]	
		Unlawful access to the air traffic control tower [D1.4:2.1] by terrorists to interfere with or control air traffic operations compromising flight safety and operations.		
	Both	Social aspects of scenarios	Media analysis and acceptance of security measures by airport passengers [D1.4:2.2, D4.2]	
ELECTRIC GRID	Strategic	Which type of regulatory structure would best incentivise and equip CI operators to be information and cyber secure?	• Economic models of the sustainability and resilience of a CI [D2.4:3.1, D6.2] facing 'shocks' to such properties. • Systems-based modelling of the agility of the CI operator to make security investment decisions in response to the regulatory structure and cyber attacks [D2.4:3.1, D6.2]	• Subject matter experts, and • media analysis [D2.4:4]
		What are the different societal views of the information and cyber security of CI and its operators?	Media analysis of the different perceptions of Stuxnet in different countries [D2.4:3.2, D4.3, D4.4].	
TR	ati	Salience and acceptance of	• Media analysis of the salience	• Workshops,

		security measures [D3.4:2.3]	and acceptance of security measures [D3.4:4, D4.3]. • Analysis of operator security and passenger complaints data [D3.4:4, D4.3]. • Social model of the effect of security measures on customer acceptance and operator’s costs and profit [D3.4:4]	• direct observation, • media analysis [D3.4:4]
		Fraud due to un-civic and antisocial motivation [D3.4:2.3]		
		Fare evasion [D3.4:2.3]	Adversarial Risk Analysis model [D3.4:2.3, D5.2]	
		Pickpocketing [D3.4:2.3]		

6. Toolkit Implementation

SECONOMICS provides a toolkit to support policy decision-making at both the operational and public level and comprises three modules:

1. The Security Problem Structurer
    - Provides an interface to build the security decision-making problem and choose a basic set of research models that will be applied to the specific security context,
2. The Security Problem Modeller
    - Sorts and determines the various parameters needed to solve the security problems. This is accomplished by:
        - identifying the relevant indicators,
        - determining the objectives for the defender,
        - integrating the risk perception of the wider public, and
        - determining the distribution of strategies for the attacker’s actions.
3. The Security Problem Solver
    - finds the optimal security resource allocation.

The toolkit was designed [D8.1, D8.2 and D8.3], implemented [D8.4] and validated [D8.5] during the lifetime of the project. SECONOMICS also developed, in the context of the toolkit, a method for producing infographics for the project’s models [Plan of info graphics design and realization]. Such infographics represent a way to show the complexity underlying the models and scenarios in a user friendly way that allows readers to capture quickly a comprehensive and thorough comprehension of the problem.

7. On-going Activities

The project is still active and will add new models to the SECONOMICS Framework, more specifically:

- a comparative and quantitative analysis of security and acceptance of risk [D4.5],
- general methods for security risk analysis [D5.3],
- a set of policy papers [D6.4],
- the validation of the tool in the case studies [D1.5, D2.5, D3.5, D8.4, and D8.5], and

- consolidation of the case studies and generalisation of the SECONOMICS Framework [D7.4].

8. Summary

The SECONOMICS Framework provides recommendations suitable for a broad range of critical infrastructure security needs. The reliability of the results has been verified through a comprehensive validation process for the specific project case studies. The models offer valuable support for those responsible for selecting the most appropriate security measures and strategies across the CI security domain. A major innovation is that the models take into account the socioeconomic context and implications. Citizens are impacted by security decisions at the supra-national, national, regional government and corporate levels. Determining the preferences of citizens is a complex task and this aspect is comprehensively analysed within the SECONOMICS project.

A further innovation is in the explicit treatment of strategic antagonists generating security threats. This strategic element is accomplished by use of decision trees and extensive game theory analysis. An insight into the public and operational policy problem in the presence of strategic attackers is essential for dealing with future and emerging threats. Historical data on the frequency of attacks is context specific and designing security policies around this evidence may lead to inefficient allocations and increase risk.

The various horizontal (across case studies) and vertical (across modelling strategies) approaches within SECONOMICS are supported by a broad set of software tools and appropriately specified infographics.

In summary the SECONOMICS project Aggregate Framework has been comprehensively validated against the project case studies. The remaining work of the project will focus on the usability of the SECONOMICS toolkit and applying the aggregate framework to case studies outside of the core case studies from within the project. The SECONOMICS project has fulfilled an ambitious task of providing a broad set of tools for modelling CI security and assisting in the analysis of public and operational policy.

REFERENCES

[D1.4] Airport Model Validation

[D2.4] National Grid Model Validation

[D3.4] Urban Transport Model Validation

[D4.2] Report on perception of security and acceptance of risk

[D4.3] Communication patterns and effective channels of communication

[D4.4] Discourses and justifications of security and risk

[D5.1] Basic models for security risk analysis

[D5.2] Case studies in security risk analysis

[D6.1] A general systems model architecture

[D6.2] Law and Economics

[D7.1] Validation Plan

[D7.2] Critical Infrastructure User Requirements

[D7.3] Aggregate SECONOMICS Framework

[D8.1] Requirements and Interface

[D8.2] Complete Design of Prototype

[D8.3] Complete Design of Prototype: Security Problem Modeller