SECONOMICS

D7.4 – Case Study Consolidation and Generalization of SECONOMICS Framework

A. Couce Vieira, S. Randall, S.H. Houmb (SNOK). R. Ruprai (NGRID), R. Munne (ATOS), Z. Mansfeldová, P. Guasti (IS AS CR), J. Williams (UNIDUR), M. Collison (UNIABDN), D. Rios, J. Cano, E. López (URJC), F. Massacci (UNITN)

Pending of approval from the Research Executive Agency - EC

Document Number	D7.4
Document Title	Case Study Consolidation and Generalization of SECONOMICS Framework
Version	1.0
Status	Final
Work Package	WP 7
Deliverable Type	Report
Contractual Date of Delivery	31.01.2015
Actual Date of Delivery	31.01.2015
Responsible Unit	SNOK
Contributors	SNOK, NGRID, ATOS, IS AS CR, UNIDUR, UNIABDN, URJC, UNITN
Keyword List	SECONOMICS Toolkit, SECONOMICS Exploitation Model, SECONOMICS Scientific Models, Generalization, Impact
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
	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	30/05/2014	Draft	S. Randall (SNOK) A. Couce Vieira (SNOK)	Instantiation of the policy insights from deliverables prior to M30
0.2	25/11/2014	Draft	A. Couce Vieira (SNOK) S.H. Houmb (SNOK) R. Ruprai (NGRID) R. Munne (ATOS)	Writing a draft with the approach to final version Revision of the policy insights instantiation
0.3	21/01/2015	Draft	E. Chiarani (UNITN)	Quality check completed
0.4	26/01/2015	Draft	A. Couce Vieira (SNOK) Z. Mansfeldová (IS AS CR) P. Guasti (IS AS CR) J. Williams (UNIDUR) M. Collison (UNIABDN) D. Rios (URJC) J. Cano (URJC) E. López (URJC) F. Massacci (UNITN)	Writing a draft based on the approach agreed in Rome GA: description of the Toolkit, policy questions and potential application beyond the project, support to toolkit development, and impact achievement
1.0	31/01/2015	Final	A. Couce Vieira (SNOK) S.H. Houmb (SNOK) F. Massacci (UNITN) E. Chiarani (UNITN)	Second quality check and refinement of the final version

INDEX

Executive summary

The SECONOMICS project has produced a Toolkit for conducting security policy analysis across critical infrastructure, allowing policy-makers to assess and optimize security policies in a structured and evidence-based process and, therefore, make better-informed policy decisions or gain insight on what makes a current security policy work or fail. In addition, the SECONOMICS Exploitation Model provides a good practice for the introduction and use of the Toolkit by policy-makers.

The scientific models developed during the project were designed to include socioeconomic aspects in the assessment of security policy-making such as the acceptance of security measures, security in the media, the effects of the different regulatory settings in security investments, security training incentives, and the optimization of the security portfolio to protect against intelligent threats. Most of the models have been integrated into the Toolkit, and their application to the case studies have adequately led to a series of recommendations to policy-makers that are of general interest, also outside of the project consortium.

The SECONOMICS Framework was developed as part of the project to address a series of policy questions relevant across critical infrastructure protection:

- Comparison of the different policy and regulatory configurations (e.g., risk-based vs rules based, centralized vs decentralized financing, customized vs uniform regulation, subsidies, insurance as a tool of public policy) and identify which approach is the better in what situations.
- Assessment of the security perception and debate in the society and what affects the final results of security policies (e.g., the acceptance of security measures and perception of threats, how the different actors shape the security debate, and the tension between security and freedom and privacy). Provide recommendations to European institutions to make this debate more interactive and participative.
- Outline effective portfolios of security measures for different threats relevant across critical infrastructure (e.g., unlawful access to critical systems, cyberattacks, petty crime, networked infrastructures).

The SECONOMICS Framework and Toolkit have been developed following the Exploitation Framework to support the Toolkit development and validate both the Scientific Models and the Toolkit. This report focuses on the generalization of the SECONOMICS framework to other critical infrastructure domains, such as Oil and Gas.

1 Introduction

SECONOMICS is a collaborative research project on the socioeconomics 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), security of critical infrastructure (the UK's National Grid), and security of public urban transport (Barcelona's urban transportation). 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 socioeconomic methodology that spans across different domains in order to support decision-making processes on the viability of security measures, taking into account the impact on citizens. The case studies (WP1, 2 and 3) provide input and validated the security models developed by the scientific work packages (WP4, 5, and 6). WP7 and 8 then integrated those results into the SECONOMICS Framework and Toolkit respectively.

The current document synthetises the Consolidation and Generalization of the SECONOMICS Framework and Toolkit that has been developed during the project.

The remainder of the document is structured as follows:

SECONOMICS Framework and Toolkit	Description of the main developments of the project: The SECONOMICS Toolkit, the Toolkit Exploitation Model, the Scientific Models, and the Information
Policy Questions	Synthesis of the policy questions and insights obtained in the project, and description of potential new scenarios on which the SECONOMICS Toolkit can be applied
Development of the Framework and Toolkit	Description of the development work of the project that led to the final SECONOMICS Toolkit and Models
Achieving the Impact	Description on how the SECONOMICS developments have achieved the expected impact
Conclusion	Concluding remarks

2 SECONOMICS Framework and Toolkit

The SECONOMICS project has developed a set of practices, models, tools and recommendations for the application of scientific models in security policy-making. The advantage of the SECONOMICS framework is that it considers the technological, social and economic aspects that together define the context of security policies at public and operator level.

More specifically, SECONOMICS have produced four main results:

- **SECONOMICS Toolkit:** Computer application for conducting security policy analysis.
- **SECONOMICS Toolkit Exploitation Model:** Good practice to effectively implement the SECONOMICS Toolkit.
- **SECONOMICS Scientific Models:** Security and socioeconomic scientific models developed during the project and integrated in the Toolkit.
- **SECONOMICS Information:** Recommendations to policy-makers and analysis of relevant security topics.

2.1 Toolkit

The SECONOMICS Toolkit is a computer application for conducting security policy analysis. The Toolkit runs scientific models specifically designed to analyse security scenarios and policy decisions relevant across critical infrastructure. These underlying models encompass socioeconomic aspects and interactions, which are paramount to understand the entire ramifications of security problems and policies.

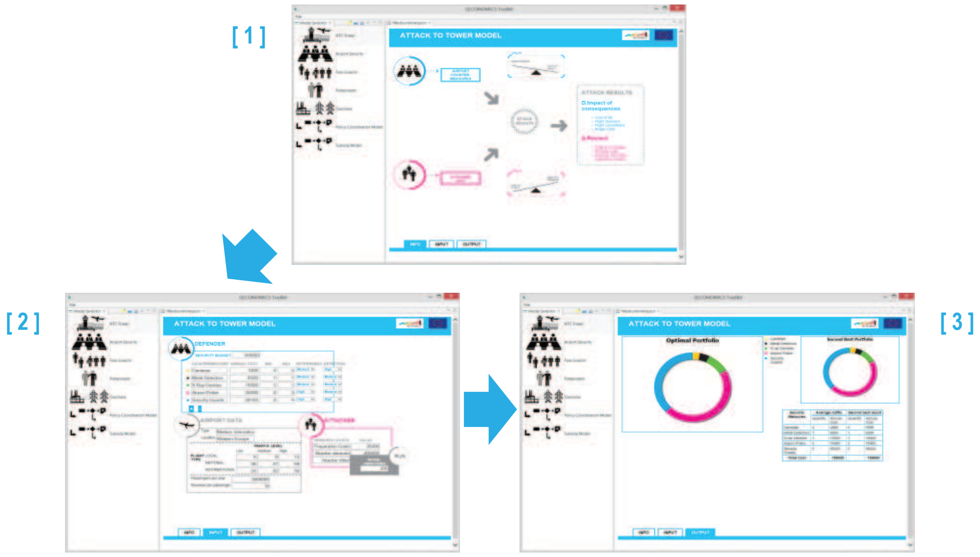

Figure 1 - SECONOMICS Toolkit: The Integrated Toolkit Framework provides a user-friendly representation of the Computational Models (based on Infographics) and an interactive step-by-step analysis: contextualization [1], input of parameters [2] and results [3].

The toolkit has four components:

- **Computational Models:** Implementation of the SECONOMICS Scientific Models as computational models. These models are implemented in Matlab, a widely used and powerful mathematical software, and compiled in Java. The Toolkit contains 6 models (their correspondent scientific models are explained in section 2.3):
    - **Attack to the Air Traffic Control Tower of an Airport:** Adversarial Risk Analysis to select the best portfolio of security measures against a terrorist threat to an air traffic control tower of an airport.
    - **Fare Evasion in the Metro**: Adversarial Risk Analysis to select the best portfolio of security measures against fare evasion in the metro system.
    - **Pickpocketing in the Metro**: Adversarial Risk Analysis to select the best portfolio of security measures against pickpocketing in the metro system.
    - **Policy Coordination of Airport Security**: Analysis of public policy decisions to select the best policy or regulatory strategy to incentivize airport security investment in both small and large airports.
    - **Policy Coordination in Electricity Network**: Analysis of public policy decisions to select the best policy or regulatory strategy to incentivize security investment in the electricity transmission and with heterogeneous operators.
    - **Subsidy and Incentives Model**: Analysis of the effectiveness of subsidy and regulatory framework (rules-based or risk-based) to incentivize CNI operators to meet a certain security assurance level.

- **Infographics:** Clear and informative representation of the Computational Models (e.g., parameters, consequences, context, steps of the analysis). The integration of the Infographics in the Toolkit interface allows users to quickly understand the scenario information and the analysis rationale. Since this information is usually complex, infographics help users to have a better awareness and control of the assessment they are performing.
- **Integrated Tool Framework:** Application that provides the necessary functionalities for running a security assessment with the Computational Models. It is implemented as a Java Program and has three main components:
    - **Analysis Plugin Provider:** Background loading of the Computational Models
    - **Selector View:** Visual component that presents a list of the available Computational Models.
    - **Parameter Input and Output View:** User interface for interacting with the Computational Models. The Infographics of each Computational Model are represented in this component and they provide information about the Model. In the Parameter Input, several elements embedded in the Infographic allow users to insert or select the parameters to run the Model. The Output View provides an Infographic with the results of the analysis. These representations are implemented as HTML and the interaction with the Computational Models (Matlab Connection) as JavaScript.
- **Matlab Connection:** Provides the connection between the Integrated Tool Framework (where users interact with the models) and Matlab (where the models run). Once the users provide the input using the Integrated Tool Interface, Matlab or Matlab Compiler Runtime can run the Models and provide the results back to the Integrated Tool Interface.

The effective use of the Toolkit allows policy-makers to assess and optimize security policies in a structured and evidence-based process and, therefore, make better-informed policy decisions or gain insight on what makes a current security policy work or fail. The knowledge generated using the Toolkit is also useful beyond the policy decision-making stage. First, the knowledge reduces the uncertainties about the security policies, allowing more control of the risks inherent in their implementation. Second, the information can be valuable for supporting policy decisions implementation, or even to support managerial or day-to-day actions once the policy is implemented. *D8.4 - Complete Implementation of Toolkit* provides a more detailed technical description of the Toolkit.

2.2 Toolkit Exploitation Model

The SECONOMICS Toolkit Exploitation Model is a good practice to effectively implement the Toolkit. The process helps introduce the Toolkit to policy-makers and is used for evidence-based policy making. These practices were successfully used and proved during the validation of the Toolkit and its models. In a more general sense, the Exploitation Model can be applied as a good practice for the introduction and use of scientific models by policy-makers.

The SECONOMICS Exploitation Model has four stages:

1. **Stakeholder Buy-In**: The first step is the introduction of the Toolkit to the stakeholders, describing the aim and functionality of the Toolkit and underlying models. This step helps to engage the stakeholders to participate in further steps.
2. **Confidence Building**: Once the toolkit is introduced, there is a need of continuous interaction with the stakeholders, through meetings and other communication channels, until they are fully familiarised and confident with the Toolkit and its models.
3. **Calibration**: Once the full familiarisation and confidence are achieved, the collaboration between the Toolkit experts and the policy stakeholders reach a state in which the Toolkit can be effectively calibrated and adapted to the particular industry or scenario considered. Important actions in this stage are the identification of the scenario parameters, and the selection of the parameters controlled by the stakeholders.
4. **What-If Scenarios**: After the calibration, the Toolkit is ready to carry out the analysis of the scenarios and provide, to the experts and stakeholders, evidence-based support for assessing the scenario and policies under study.

The Exploitation Model allows the use of the Toolkit by industry stakeholders with the support of a consultant with expertise in the SECONOMICS Toolkit. Together, they are in a position to successfully apply, adapt and calibrate the security models for new uses or scenarios. The Toolkit Validation deliverables [D1.5, D2.5, and D3.5] contain a more detailed description of how the SECONOMICS Exploitation Model was used in each case study to validate the Toolkit and the Scientific Models.

2.3 Scientific Models

The SECONOMICS Scientific Models are the security and socioeconomic models developed in the project. The Scientific Models structure the social preferences and economic incentives of the agents (e.g., public, organizations, governments, attackers) within the specific physical and technological context of the security scenarios addressed. Security decisions – even at operational level - have a public component since institutional arrangements and public perception have an important effect in the success of security policies. Additionally, risk assessments should include the analysis of the users and attacker behaviour to optimize risk management measures.

The integrated use of the models allows the study of the socioeconomic aspects of security policy-making, including risk and implementation aspects. Public policy is implemented by legal instruments designed to maximize social welfare, whereas operational policies are designed to minimize risk and comply with the mandatory regulations. The objectives of operational policies and public policies usually differ, mainly for two reasons: operators and the society have different preferences, and externalities (i.e., cost or benefit caused to third-parties) alter the cost assumed by each of them. On the other hand, the relevancy of social preferences in security policy is twofold. First, policy makers have to include the public preferences towards threats and security measures into their security policy objectives. Second, it is important to consider the way users and employees react to security measures, and how this reaction affects the efficacy of operational security measures. The design of security policies in this setting is complex, and may result in well-intentioned policies that fail in their implementation or cause more problems than they solve. Another important challenge is the presence of trade-offs (e.g., security vs freedom).

The integral approach of SECONOMICS is defined in the ***Model of the Political Economy of Security Risk Management*** [D6.4], which examines security as a public gods and how this can be modelled to help a social planer design a secure environment. This model unifies security, social, political and economic concepts into a synthetic model. Although the focus of the paper is a Public Policy Model, its paradigm spans to all of the Scientific Models of SECONOMICS, and it is the foundation of how they are integrated.

Scientific Models:

- **Model of Public Acceptance of Security Measurers:** Analysis of the effects of security measures on passengers in aviation and urban public transportation. The Model provides input to the Public Policy and Risk Models to help define the impact of security measures on citizens and users.
- **Coding Technique for Salience Analysis in the Media**. Model to code in a semi-automated way media artefacts (e.g., printed, online and social), allowing a structured analysis of a relevant topic in the public debate. The Salience Analysis concepts and input have been integrated into the Public Policy Models, to define the public preferences and risk perceptions that configure security as a public good. The Coding Technique is designed for three security domains (aviation, urban public transport and CNI) but it can be applied, with some adjustments, to other domains.
- **Models for Public Policy with Mandatory and Risk-Based Security Investments:** Game-theoretic model to analyse the subsidy and regulatory framework (rules-based or risk-based), taking into account the reaction of both operators and attackers to the regulation, and the presence of shocks with impact in security.
- **Models for Public Policy for Security Investments with Heterogeneous Industries and Network Effect:** Game-theoretic model that shows how policy or regulatory strategies affect the particular security investments for operators differently. The model also considers attackers, security externalities (e.g. security investment in one airport may increase security in others), and technological changes. The differences are based on the specific characteristics of the operator (size, exposition to threats) and the level of interconnection between operators.
- **Incentives for Security Training:** Public Policy Models and studies to help the selection and implementation of security training by considering the trade-offs and objectives of the trainer, and the motivations of the trainees. The base is a Principal-Agent model where the Agent (policy or security staff) makes a decision on behalf of the Principal (security planner). It also provides the base of the investment functions used in the previous two Public Policy Models.
- **Public Policy and Cyber Insurance:** General public policy and security model with reactive threats, and with the inclusion of assurance and insurance components. It takes into account the risk appetite of the agents, and the presence of externalities and attackers with strategic behaviour. It can be used to study how firms and individuals interact in the presence of security threats, and to design policy assurance and regulatory or subsidy mechanisms. It is the mathematical base of the previous three Models, and shares the use of the concepts of risk

aversion and utility to model the evaluation of the security risk with Adversarial Risk Analysis.

- **Adversarial Risk Analysis for protecting one site:** Risk analysis model that helps organisations to select the optimal portfolio among different security measures. It takes into account the forecasting of the strategic behaviour of the attacker, the risk attitude of the defender, and the uncertainties of the scenario. There is a set of models, each one with different patterns of attacker-defender interaction, or for the modelling of scenarios with several attackers or several defenders.
- **Adversarial Risk Analysis for protecting several sites:** ARA for selecting the optimal portfolio among different security measures to protect independent sites, spatially related sites, and a network of sites.

One of the findings in the project was that it was more convenient to implement most of the models in the Toolkit to carry out their validation (moreover, the final model validation was done together with the Toolkit validation). Other models provided good results analytically, without the need to implement them into the toolkit. The scientific deliverables provide more detailed information about the specific Models on the Security and Society Models [D4.3, D4.4 and D4.5], the Public Policy Models [D6.1, D6.2, D6.3, and D6.4], and the Adversarial Risk Analysis Models [D5.1, D5.2, and D5,3]

2.4 Information and Analysis

The SECONOMICS Information consists of recommendations to policy-makers and analysis of relevant security topics. The project has generated evidence-based data, analysis and policy recommendations through research and validation with the stakeholders. Great part of this information was used during the project to build the security scenarios, but above all, the information provides useful insights to all those interested in critical infrastructure security. More specifically, the series of analysis and recommendations is listed below:

- **Media Analysis of Security Perception by Citizens**: Analysis on the perception of security issues in printed, online and social media across Europe and other countries, as well as surveys with end-users in the Aviation domain.
- **Media Corpus:** Collection of articles on three relevant security issues that can be used for further research and analysis. Closed Circuit Television (CCTV), 3D Body Scanner and the Stuxnet cyber attack. More than 2800 articles in 10 languages, covering a period of 40 months (2010-2013).
- **Recommendation on Public Policy for Security:** The research of the project has generated a set of evidence-based policy advices and insights with special focus on communication, European coordination in critical infrastructure security, and future and emerging threats. Section 3 summarizes some of these insights.

3 Policy Questions

Table 1 in the next pages provides a synthesis of the policy questions and topics addressed during the SECONOMICS project. From the beginning of the project, several policy questions and challenges have been identified across the case study domains to set the basis of the project work and define the security scenarios and models that would eventually provide insights into them. The policy questions have been structured into three levels:

- **Strategic**: challenges at the regulatory and public policy level.
- **Citizens**: challenges related with the social perception of security issues by citizens and users.
- **Operational:** challenges related with the selection of security measures at operator level.

The second column in the table lists the policy questions and the associated deliverables that describe the activities and models addressed in each question. The third column provides a synthetic description of the policy insights that the application of the SECONOMIC Framework and Toolkit has generated in respect to the policy questions, with a reference to the deliverables that contain the full recommendations and insights for each question/topic.

In addition, the *Potential Application* columns show relevant security scenarios where the SECONOMICS Toolkit can be applied. Specifically, new scenarios in the domains of the project (Airport, CNI and Public Transport) and scenarios in a new domain (Oil and Gas) based on security topics in this domain in which the relevancy of socioeconomic aspects models represent and opportunity to further apply the SECONOMICS Framework and Toolkit.

Table 1 – SECONOMICS policy questions and topics

Level	Deliverable - Policy Question/Topic	Policy Insight [Deliverable]	Potential Application in SECONOMICS domains	Potential Application in new domain: Oil and Gas
Strategic	**D2.5, D6.2. D6.4 - Which type of regulatory structure would best incentivise and equip CNI operators to be information and cyber secure? (CNI)**	Risk-based regulation provides more efficient security investments, flexibility and agility. However, the operator needs to meet a certain level of security and awareness maturity. Rules-based regulation provides to the regulator assurance that certain level of protection is in place. However, it may lead the operator to reduce security investments. [D6.4] The model suggest a careful framing of the policy, since the answer is sensitive to the problem context. In general, the best solution is a mixed system that combines the benefits from both rules-based and risk-based approaches: A rules-based regulation could apply to CNI operators below a certain level of maturity in their security, and a risk-based regulation could apply to those operators above a certain maturity level (e.g., those with an established risk management framework). [D2.5, D6.4]	Assessment of the risk-based and rules-based regulatory frameworks to find which one best incentivise drone commercial operators of unmanned aerial vehicles to achieve an optimal security level (Airport)	Assessment of the risk-based and rules-based regulatory frameworks to assess the introduction of NIST Cybersecurity Frameworks, and how it may affect cybersecurity posture in O&G
Strategic	**D1.4, D6.3, D6.4 - Effective airport security regulations to incentivize airports to invest in security measures at a social optimal level (Airport)**	The presence of the externality effect of security expenditure makes that the outcome of a specific regulatory and financial policy for airport protection depends on the degree of interdependence between the airports; specifically a combination of both centralized and decentralized financing will result in a better social outcome than either centralized or decentralized financing alone. Even so: 1. If the interdependence is low, decentralized financing with a customized regulation is likely to lead to an optimal social outcome. 2. If the interdependence is high, large airports tend to under invest in security. In this case, a uniform regulation is likely to provide a better social outcome than a customized regulation. [D1.4, D6.4]	Study of the regulation and financial policy to best incentivise security investment in the electricity transmission with heterogeneous operators (CNI)	Effective security regulations for O&G platforms to incentivize the companies involved in the operations (several per platform) to invest in security measures at a social optimal level
Strategic	**D6.4 - Fair and efficient cost sharing of security for aviation and CNI. Mandatory vs Voluntary security investment**		Pan European cooperation on petty crime. Future iterations NIS Directive (which at the moment is voluntary, but it may shift)	Analysis of the shift from voluntary approach to an overseeing approach that occurred in the North Sea during the 80s (in response to several accidents)

Level	Deliverable - Policy Question/Topic	Policy Insight [Deliverable]	Potential Application in SECONOMICS domains	Potential Application in new domain: Oil and Gas
Strategic	**D6.4 - Effective management of training activities accounting for incentive incompatibilities in principal-agent interactions**	The contract with the security employee should be based on compliance with rules rather than on performance during security breaches (since they are rare events). It should be also considered job satisfaction, peer recognition and, especially, education and training. The effort and performance in training is related with the commitment of the employee to his position and to future employability. Technical training increases the trainee employability and represents a situation in which he can demonstrate his abilities; it also provides a better understanding than the more abstract general training. If the training has consequences (rewards and penalties), the employee will be more engaged in the activity. [D6.4]	Training of Industrial Control Systems operators and engineers to account for the evolving cybersecurity threats	Training of Drilling Control Systems operators and engineers to account for the evolving cybersecurity threats. Assessment of the Whistle-blower policy in from a Principal-Agent point of view, e.g., the whistle-blower as agent and the company as principal.
Strategic	**D6.4 - Cyber Insurance as a tool of public policy? (CNI)**	Public policy is needed since any form of insurance reduces security investment but does not provide a reduction in the aggregate risk. [D6.4]	Assessment of insurance as public policy tool for industrial control systems cybersecurity (general and cross-sector)	Assessment of insurance as a tool of public policy for drilling control systems (instantiation of the former to particular systems and installations)
Strategic	**D6.4 - Subsidies for regulated CNI organisations? (CNI)**	In the case of energy the rates of the electricity place should be large enough to ensure that security investments are met, but short enough to minimize the cost to society. [D6.4]	Analysis of the subsidies and how they affect security investment in other regulated utilities (e.g., airlines, water, telecommunications)	Analysis of taxation and how it affects security investment in O&G
Strategic	**D4.5, D6.4 - Pan European public policy mediated information sharing and training**	European institutions have the opportunity to shape the public debate on security in the media and transform it into an interactive discussion, by implementing the following actions: • Promote independent, critical and accessible news sources at the European level *(continued on the next page)*	Managing emerging externalities connected to Freedom of Movement. Evolution of the European Arrest Warrant and EC Cyber Directive. Metadata collection and sharing within the boundaries of EU Law	Evolution of ENISA responsibilities. Pan European coordination on HSE. Capability maturity exercises

Level	Deliverable - Policy Question/Topic	Policy Insight [Deliverable]	Potential Application in SECONOMICS domains	Potential Application in new domain: Oil and Gas
Citizens	**D4.3, D4.4, D4.5 - Plurality of media commentary, inclusiveness of security debate, and participative character**	• Encourage the participation and approval of underrepresented voices such as citizens, civil right groups and security experts • Facilitate critical debate between opponents and proponents of security measures These actions require European institutions to exploit new media platforms, such as blogs and social media, and cultivate communication channels with traditional media. [D4.4, D4.5]	Security and privacy in Social Media and liability and civic responsibility for social media stakeholders	Transparency of O&G activities to the public
Strategic and Citizens	**D.4.3, D4.4, D4.5 - Targeted communication strategy to ensure that firms and citizens are informed on security risks, measures, and their rationale**	Media, as information transmitter and public opinion maker, is in position to highlight the importance of balancing between freedom and security: • When planning to introduce a new security technology, authorities should consider salience and social perception and attitudes towards the new security. • New measures can introduce new public concerns based on media salience and social behaviour (e.g., personal views on what is an acceptable body search). These concerns can outweigh the security benefits of the security measures. • The development and implementation of new security policies have to take into account the lack of understanding of emerging threats and what constitutes safe behaviour. [D4.3]	Analysis of further topics: • Security challenges of globalisation and growing diversity • Society going forward has increased dependency on the security of individual citizens • Growing need for shared responsibility	Analysis of the role of communication on preventing and handling critical security incidents in O&G installations

Level	Deliverable - Policy Question/Topic	Policy Insight [Deliverable]	Potential Application in SECONOMICS domains	Potential Application in new domain: Oil and Gas
Citizens	**D2.4, D3.4, D4.3, D4.5 - Acceptance of security measures (Airport, Public Transport)**	The perception of the effectiveness and value of a security measure increases the acceptance of this measure. In order to improve the perception and acceptance of security measures, it is important to: • Consider the relative importance of security measures when training personal • Explain the importance and rationale of security measures to users/citizens • Recognize user concerns with security measures and cultural differences and social factors • Consider the perception of the measures as both legal and legitimate Main differences between countries: • Countries more active in the international scenes, or with terrorism experiences, are more concerned with security measures, whereas less exposed countries are more concerned with the cost of security measures • Security incidents in which a security countermeasure has proven successful boost temporarily the acceptance of the measure in that country, but after a while, media and cultural attitudes remain the main source of acceptance. [D3.4, D2.4, D4.3, D4.5]	Application of the analysis of the acceptance of security measures to other forms of mass transport vulnerable to security threats (e.g., high-speed train)	Application of the analysis of the acceptance of the security measures, by personnel and visitors, in an O&G platform or installation
Citizens	**D3.3, D3.4, D4.3, D4.4, D4.5 - Feeling of Security in Metro (Public Transport)**	In the case of un-civic and antisocial behaviour in public transport, pickpocketing is the largest source of incidents reported to the police and it has a twofold media impact: on feelings of insecurity in the city, and in bad reputation of the city in foreign media. Un-civic behaviour and fare evasion do not represent major concerns to passengers. [D3.4] Increase of pan-European coordination to fight pickpocketing as organised crime, always in accordance with the European principles of freedom of movement and Europe without borders. [D4.5]	Assessment of the security feeling in other topics: • Online security awareness and illiteracy • Feeling of security in the online public sphere and spaces • Fear of fraud, cyber bulling and other antisocial behaviour	Assessment of the security feeling in relation with: • Surveillance of O&G platform staff • Cyber espionage • Bring-your-own-device policy

Level	Deliverable - Policy Question/Topic	Policy Insight [Deliverable]	Potential Application in SECONOMICS domains	Potential Application in new domain: Oil and Gas
Citizens	**D4.5 - Trade-offs between security and freedom, privacy, health/well-being and costs**	Existence of trade-offs between security and health, privacy, freedom and costs. In all the security measures assessed, the tension between freedom and security is clear. They affect the perception of security by citizens and, therefore, policy makers should balance the implementation of security measures with their impact on citizens' rights. The media has a key role in shaping this debate. Especially as a counterpoint to the tendency of governments towards over-security. [D4.5]	Analysis of the trade-offs between privacy and security in online activities (e.g., nation-state security surveillance). Protection of the freedom of speech and protection of whistle-blowers	Analysis of the security trade-offs involved within the trade-off between corporative interests and public interests. Protection of corporate whistle-blowers.
Citizens	**D2.4, D4.3, D4.5 - What are the different societal views of the information and cyber security of CNI and its operators? (CNI)**	Citizens underestimate the relevancy of CNI cybersecurity. It does not involve them directly, but it is a national security topic with the potential to cause citizens direct or indirect security costs. There should be a broad debate on CNI cybersecurity and a proactive information strategy. [D2.4, D4.5]	Assurance and reliability of information for future and emerging CNI threats and appropriate dissemination of sensitive information	Same as CNI
Operational	**D1.3, D1.4, D1.5 - Effective risk portfolio strategy for protecting against unlawful access to sensitive areas by terrorist to take control of the systems, installations and operations (Airport)**	Insights on the tactical behaviour of a terrorist group trying to take control of the air traffic control (ATC) tower. Although terrorist are considered risk-seekers, they will only put themselves at risk if they think they have a chance to cause significant disruption to airport operations. When specifying policies and measures to counter a terrorist attack on an air traffic control tower, it is worth considering that in such a case terrorists would tend to; 1. deploy few terrorist if they think that the security measures are very strong 2. deploy as many terrorist as they can if they think that the infrastructure is vulnerable, and, 3. opt for an intermediate strategy if they have any doubts [D1.4]	Analysis for protecting against a terrorist attack or sabotage in a substation access (CNI) or underground control center (Public Transport)	Analysis for protecting against a terrorist attack or sabotage in refinery, pipeline or other land-based installation

Level	Deliverable - Policy Question/Topic	Policy Insight [Deliverable]	Potential Application in SECONOMICS domains	Potential Application in new domain: Oil and Gas
Operational	**D1.3, D1.4, D1.5, D5.2, D5.3 - Effective risk portfolio strategy for protecting against a cyberattack with impact in operations**	Recommendations for dealing with a cyber-threat that could have an impact on airport operations: 1. Invest on the most effective security measures, even if they are the more expensive ones, in order to counter threats from highly skilled hackers 2. Invest in a wide range of measures, even if they are not the most effective ones, in order to cover as many areas as [possible that might be attacked by inexperienced hackers [D1.4]	Analysis for protecting against cyber attacks to the electric transmission control systems (CNI)	Analysis for protecting against cyber attacks to a drilling control system in a drilling platform (D5.3)
Operational	**D3.3, D3.4. D5.2, D5.3 - Effective risk portfolio for protecting against petty crime at urban transport (fare evasion and pickpocketing)**	Organized crime, in the case of pickpocketing act with cost-minimizing strategies and adaptive intelligence, working transnationally by taking advantage of local laws and regulations. The deployment of personnel is the most effective measure for countering fare evaders and pickpockets, more specifically: 1. Inspectors with inspection and collection powers are effective in combatting fare evasion in a single station. 2. Patrolling Inspectors with their overt deterrent effect are an excellent measure for fighting both fare evasion and pickpocketing in a single station when used in conjunction with CCTV. [D3.5, D5,2, D5.3]	Analysis for protecting against pickpocketing in airports	Analysis for protecting against non-authorized access to corporate buildings or industrial installations
Operational	**D5.3 - General models for selecting an effective risk portfolio considering infrastructures with multiple nodes in a network**	Inspectors, patrols and ticket clerks involved in observation tasks are together the most effective measure for fighting fare evasion and pickpocketing in multiple stations, particularly when used in conjunction with automatic access doors. [D3.5, D5,2, D5.3]	Analysis for protecting against: • Petty crime at several metro stations (Public Transport). • Sabotage in grid remote installations (CNI) • Terrorist attack in railway system (D5.3)	Large-scale cyber-attack to the entire installations of a company or an entire critical sector, perpetrated by a nation-state during an escalated conflict.

4 Development of the Framework and Toolkit

Stakeholder Buy-In

Identification and engagement of case study domain stakeholders at national, European and International level in the case study domains of Airport (ENAC, ACI-Europe, Eurocontrol, IATA, Assoaeroporti), CNI (National Grid's, CPNI, ENTSO-E, UK Cabinet Office, DECC), and Urban Transport (TMB, Mossos d´Esquadra, UITP) has been crucial for stakeholder buy.in. The participation in conferences, events or specific meetings and dissemination workshops helped to present the project and gain the buy-in of these stakeholders. The first and second stakeholder´s report [D9.8, D9.13] provide more detail on the community building activities that have been used to gain the stakeholder buy-in and to build their trust.

Establishing Trust

Building the trust in the SECONOMICS methodology, and specifically, the Models and Toolkit was achieved through activities such as presentations, training and analysis to explore the aims of the project and the scientific background, evaluation of the potential of the Toolkit and the Models in the selected domain, and discussion of what can be answered using the Toolkit and what cannot. These activities helped to engage the stakeholders and get them to contribute to the Toolkit development (i.e., sharing data and information for calibration, discussion and validation of the final what-if scenarios).

Calibration

Calibration of the Toolkit and the Models to the specific requirements of the domain and stakeholders has been essential. This step included the calibration of the scientific aspects (e.g., Scientific Models, scenarios and data) and the software/interface aspects (e.g., graphical user interface, infographics, Computational Models) of the toolkit. During the calibration phase stakeholders discussed the parameter structure of the models with the aim to calibrate them, provide the first interpretations of the Models (e.g., trade-offs, expectations), and analyse the Toolkit through expert judgements and interviews. This interaction generated a list of potential problems and recommendations to improve the Toolkit and the underlying models. The final version of the requirements [D1.3, D2.3, D3.3, and D7.2] provides a list of all the stakeholders, their mutual interactions, and their requirements. *D8.3 – Complete Design of Prototype: Security Problem Modeller* provides more detail on the Toolkit design [D8.3].

Support to Toolkit Development

The support provided by the case study experts and stakeholders to the toolkit development consisted of three stages. The first stage was the interface testing and adaptation, together with the Toolkit responsible. This stage involved the evaluation of the graphical user interface (GUI) components and the infographics by the stakeholders and experts in interface usability, employing GUI design and evaluation techniques (e.g., cognitive walkthrough, task-analysis methodology). The second stage involved the Toolkit tuning with the scientific WP (see Validation of Scientific Models below). The third stage involved the refinement of the interface and was held in parallel to the Toolkit validation workshops (see Validation of the Toolkit below).

What-If Scenarios
Demonstration and testing of the Toolkit in several scenarios, with different input values for the parameters, to check the results against the experience of the stakeholders, was the basis for developing what-if scenarios. Study on how the stakeholders used the Toolkit without guidance and how they took advantage of the Toolkit for accepting and validating the scenarios. Several validation sessions in each case, with discussions, interviews and questionnaires provided input at this stage. The validation activities and meetings, and the continuous interaction between domain stakeholders and consortium members, allowed to iterative improve the models, Toolkit, information, exploitation methodology, and the final policy outcomes of the project.

Validation
A complete validation process was implemented to verify that the functionality of the Toolkit and the Models is accurate and useful and meets the expectations of the case study stakeholders. Validation activities involved domain experts to assess the models from a practitioner point of view, and to identify expectations, user needs, and opportunities for exploitation. *D7.1 – Validation Plan* defined a validation framework with three high-level objectives: user acceptability, domain suitability, and technical usability. Each of these objectives is detailed in more refined validation criteria. The validation approach is a customized framework based on the consortium experience with other several successful methodologies (e.g., MEM, TAM, E-OCVM. User-centred evaluation methodologies, cognitive walkthrough, or expert judgement). The need of a customized framework arises from the fact that the models, toolkits and practices have to had a pragmatic value, i.e., can only be effective on the basis of applied success in practice. The validation objectives serve to measure the perceived efficacy, ease of use, usefulness, effectiveness, quality of results, technical soundness, memorability, reusability, etc. These objectives were elicited at various stakeholder meetings throughout the project lifecycle.

Validation of Scientific Models
The validation of the Scientific Models consisted of the consolidation of the security scenarios according to the stakeholders needs, and in the identification of relevant topics for research. It also involved the presentation and discussion of the models with relevant stakeholders in the domain, and then refined iteratively by the consortium partners. In addition, the project needed an extensive data gathering for supporting the model development, requiring activities such as investigation, questionnaires, interviews, media analysis, surveys to passengers and travellers. The main issues addressed during the validation of the Scientific Models were incorporating the stakeholders' decision-making processes, refining the structure and algorithms of the models, assessing whether the model fits to the domain, and the generalization and customization of the models.

Validation of the Toolkit
The validation of the Toolkit consisted of three phases. First, finalizing the validation of the Scientific Models by providing further data, evaluation of the prototypes, and the refinement of the models for being implemented into the Toolkit. It also included the mentioned support to the Toolkit development (e.g., functionalities, look and feel). Second, the internal evaluation of the Toolkit to support the definition of the scenarios

for external validation, and the interpretation and harmonization of the results provided by the toolkit. This stage involved consortium partners and case study domain experts. Third, the external validation of the Toolkit with live trials of the Toolkit with domain security stakeholders and policy makers, focusing on the final release of the Toolkit.

The validation objectives (user acceptability, domain suitability, and technical usability) were met, and there is high potential for the application of the Toolkit in other new fields, such as Oil and Gas. Meeting the validation objectives were crucial to drive the development and validation of the Toolkit. The user acceptability among the stakeholders was high. The Toolkit is well presented, memorable and easy to use, it was also fount scientifically and technical sound, reaching a high satisfaction level. On the domain suitability, the Toolkit seems capable of enabling non-expert user to apply content to their domain with documented guidelines, although the tool needs the assistance of a Toolkit expert and a domain expert to provide detailed context. On the technical usability, the Toolkit provides flexibility while remaining efficient and effective, allowing a prone usage of the underlying scientific models to carry out security assessments. *D8.5 – Consolidated Validation and Evaluation of Toolkit* provides a summary of the Toolkit validation and evaluation activities within the case studies. Specific deliverables in each case study provide more details of the Model Validation [D1.4, D2.4 and D3.4] and the Toolkit Validation [D1.5, D2.5, D3.5].

5 Achieving the Impact

Provision of a general socioeconomic methodology for security resource allocation relevant across various domains: The project has developed a general socioeconomic approach, initially defined in the scope of the project and in the paper Model of the Political Economy of Security Risk Management [D6.4], which arises from the interaction between the different Scientific Models (see section 2.3). The validation activities of the Scientific Models and the generation of policy insights in societal, public and operational policy making across the three case studies show the relevancy of SECONOMICS methodology in those domains. The semantics of the methodology is formalised, and allows stakeholders to understand the explicit links of the elements and the results of each Scientific Model. The scientific methodology can be applied to new domains and scenarios without additional R&D activities, requiring just a revision of the existing to adapt them to the new domains.

Provision of a tool that facilitates such process to policy makers: Most of the models were implemented into the Toolkit to facilitate their validation and to save human effort, although other models provided results analytically, without the need to implement them into the Toolkit. The Toolkit is fully integrated with the scientific methodology, and all the Computational Models are fully implemented as automatic and interactive algorithms that generate solid results in an acceptable time. The validation of the Toolkit was successful, since all the validation objectives were met and the Toolkit was accepted by the stakeholders (section 4).

Under the Technology Readiness Level (TRL) paradigm of the European Union, TRL-5 is defined as “technology validated in relevant environment (industrially relevant environment in the case of key enabling technologies)" and TRL-4 as "– technology validated in lab". NASA further details the definitions[1]:

> *"TRL 4 Component/subsystem validation in laboratory environment: Standalone prototyping implementation and test. Integration of technology elements. Experiments with full-scale problems or data sets."*
> *"TRL 5 System/subsystem/component validation in relevant environment: Thorough testing of prototyping in representative environment. Basic technology elements integrated with reasonably realistic supporting elements. Prototyping implementations conform to target environment and interfaces."*

The Toolkit fully integrates the Scientific Models in a stand-alone application, and the results of the validation of the Toolkit suggest that the SECONOMICS Toolkit is at TRL-5. The validation activities all along the Calibration and test of What-If Scenarios phases (see section 4) provided (1) representative and solid input from the environment to refine the models, (2) realistic generation of policy outcomes relevant to the stakeholders present in the validation, and (3) consistency with their expectations.

Showcase such methodologies and tools in relevant case studies, which may serve as best practice analysis that may be replicated in other European (and global) critical infrastructures: The selected case studies (Airport, Electric grid as CNI, and Metro as Public Transport) allowed the assessment of different security challenges and measures that are present in most of critical infrastructures (e.g., cybersecurity, terrorism, petty crime, security regulatory frameworks, citizens perception of threats and security measures, media coverage on security issues). In addition, the case studies provided input on the European security coordination within each of the domains [D1.4, D2.4, D3.4]. The interactive nature of the development and validation activities allowed that the input from each case study shaped the cross-domain applicability of the Models and the Toolkit. More specifically, section 3 shows relevant security scenarios where the SECONOMICS Toolkit can be applied, in the domains of the project (Airport, CNI and Public Transport) and in a new domain (Oil and Gas). In addition, there is a plan for the potential exploitation of the Toolkit and other results [D9.10].

Inclusion within the global risk governance process issues in relation with social perceptions and attitudes towards risk as key drivers: SECONOMICS has developed an entire work line on social and security research and models. The scientific Social Models provided valuable policy recommendations and information (e.g., Media Analysis of Security Perception by Citizens, Media Corpus). The concepts of these models (e.g., attitudes towards security measures, security preferences) were integrated in the rest of the Public Policy and Risk Models, and the research within this work line provided valuable data input to fill the Public Policy and Risk Models.

Improvement of the process of identifying and assessing risks from an economical point of view: SECONOMICS provided a wider assessment of security risks with the inclusion of socioeconomic aspects. The Public Policy Models enhance government-level risk assessment by the inclusion of social perceptions and economic behaviour in the risk

[1] http://esto.nasa.gov/files/trl_definitions.pdf

assessment. It is also important to model the regulatory frameworks to better define government "risk mitigation strategies" (i.e., policies and regulation). On the other hand, Adversarial Risk Analysis incorporates the strategic attacker behaviour into the model. Both Models also formalize risk assessment by representing risk attitudes by means of utility functions, and modelling agents (e.g., operators, attackers). The implementation of these models into the Toolkit provides an easier and use of these models.

Improvement of the process of balancing security, with policy, economics and other relevant constraints: There are multiple trade-offs in security policy (e.g., the tension between security and freedom at the social level, security public policies that provide more flexibility or assurance, risk and costs). The SECONOMICS Models help to formalize these differing objectives into utility functions that capture their preferences. With these preferences defined, it is possible to find the security policies that provide the highest social welfare.

Improvement of the process of quantifying positive and negative externalities: The scientific work of the project has identified relevant externalities related with security (e.g., the acceptance of security measures by citizens, the transference of security costs or benefits between operators of an industry). Although difficult to measure, the nature of the Scientific Models as structural models allowed for the observations and analysis of these variables incorporated as input into the Toolkit. The analysis combined research practices widely used in social sciences, but also a thorough structuration of the feedback provided by case study stakeholders to incorporate it into the Toolkit.

6 Conclusions

The effective use of the SECONOMICS Toolkit enables policy-makers to assess and optimize security policies in a structured and evidence-based process to make better-informed policy decisions and gain insight on what makes a security policy work or fail. This is achieved thanks to the integrated use of the Scientific Models, and their incorporation into the toolkit, successfully capturing the relevant socioeconomic aspects of security policy-making. In addition, the Toolkit Exploitation Model provides a process that allows the effective implementation of the Toolkit by industry stakeholders. This Exploitation process has been used in each case study to validate the Toolkit and the Scientific Models.

The project addressed a series of policy questions and topics: the application of the Framework and Toolkit has generated a set of evidence-based policy advices and insights for protecting the case study domains. These security challenges are also present in other critical infrastructures, and the document identified potential new scenarios in the domains covered by the project, as well as scenarios in a new domain (Oil and Gas industry).

Overall, the expected impact of the project and the validation objectives of the work (user acceptability, domain suitability, and technical usability) were met to a large degree. This, together with the fact that securing critical infrastructure is becoming more and more challenging, indicate the potential of the SECONOMICS Framework and Toolkit to support security policy-making.

REFERENCES

[D1.3] Airport Requirements – Final Version

[D1.4] Airport Model Validation

[D1.5] Tool Validation

[D2.3] National Grid Requirements – Final Version

[D2.4] National Grid Model Validation

[D2.5] Evaluation tools for providers and policy paper on future and emerging threats

[D3.3] Urban Public Transport Requirements – Final Version

[D3.4] Urban Transport Model Validation

[D3.5] Tool 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

[D4.5] Price of Security. Comparative analysis of public attitudes to security and acceptance of risk

[D5.1] Basic Models for Security Risk Analysis

[D5.2] Case Studies in Security Risk Analysis

[D5.3] General Methods for Security Risk Analysis

[D6.1] A General Systems Model Architecture

[D6.2] A Report On the Interaction of Systems Models and Models of Economics, Law and Society

[D6.4] A Set of Policy Papers

[D7.1] Validation Plan

[D7.2] Critical Infrastructure User Requirements

[D7.3] Aggregate SECONOMICS Framework

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

[D8.4] Complete Implementation of the Toolkit

[D8.5] Consolidated Validation and Evaluation of Toolkit

[D9.8] First Stakeholders´ Panel Report

[D9.13] Second Stakeholders´ Panel Report

[D9.10] Final Exploitation Plan