SECONOMICS

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

R. Ruprai (NGRID), D. Willacy (NGRID), P. Bamford (NGRID), J. Williams (UDUR), M. Collinson (UNIABDN), F. Massacci (UNITN)

Pending of approval from the Research Executive Agency - EC

Document Number	D2.5
Document Title	Evaluation tools for providers and policy paper on future and emerging threats.
Version	1.0
Status	Final
Work Package	WP 2
Deliverable Type	Report
Contractual Date of Delivery	31.01.2015
Actual Date of Delivery	31.01.2015
Responsible Unit	NGRID
Contributors	UNIABDN, UDUR, UNITN
Keyword List	CNI, Model Validation
Dissemination level	PU

SEVENTH FRAMEWORK PROGRAMME

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 TEDESSCHI 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) whose principal administrative office is at 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: Silvia Castellvi Catala silvia.castellvi@atosresearch.eu
8	SECURENOK	SECURE-NOK AS, Professor Olav Hanssensvei, 7A, 4021, Stavanger , Norway Postadress: P.O. Box 8034, 4068, Stavanger, Norway http://www.securenok.com/	Contact: Siv Houmb sivhoumb@securenok.com
9	SOÚ Institute of Sociology AS CR	INSTITUTE OF SOCIOLOGY OF THE ACADEMY OF SCIENCES OF THE CZECH REPUBLIC PUBLIC RESEARCH INSTITUTION, Jilska 1, 11000, Praha 1, Czech Republic http://www.soc.cas.cz/	Contact: Dr Zdenka Mansfeldová zdenka.mansfeldova@soc.cas.cz
10	nationalgrid THE POWER OF ACTION	NATIONAL GRID ELECTRICITY TRANSMISSION PLC, The Strand, 1-3, WC2N 5EH, London, United Kingdom	Contact: Dr Raminder Ruprai Raminder.Ruprai@nationalgrid.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	06/01/2015	Draft	R. Ruprai (NGRID), D. Willacy (NGRID), P. Bamford (NGRID)	Initial full draft To be completed: Table links, Appendix A, Appendix B, Appendix E – Policy Papers.
0.2	09/01/2015	Draft	E. Chiarani (UNITN)	Quality Check completed. Minor comments made and actioned.
0.3	12/01/2015	Draft	R. Munne (ATOS)	Scientific Review completed. No comments to action
0.4	19/01/2015	Draft	R. Ruprai (NGRID), J. Williams (UDUR), M. Collinson (UNIABDN), F. Massacci (UNITN)	Executive summary, Appendix B and Appendix E added and finalised
0.5	26/01/2015	Draft	F. Massacci (UNITN)	Scientific Review
1.0	30/01/2015	Final	R. Ruprai (NGRID), F. Massacci, W. Shim (UNITN)	Appendix A added and finalised. Minor changes to Executive Summary and Introduction. Dissemination Level changed to PU.

INDEX

Executive summary

This report builds on the modelling validation work in Deliverable D2.4, CNI Model validation, and presents in detail the work in the CNI case study in Year 3 of the SECONOMICS project.

Within this report the four different stages of the SECONOMICS practice of exploitation of the CNI toolkit are first defined. Following this, the 12 validation events/activities are presented which clearly and successfully validate the CNI case study toolkit's practice of exploitation. These validation event attendees included the key members of the CNI stakeholder panel, National Grid's Digital Risk & Security leadership, the UK's Centre for the Protection of National Infrastructure and European Network of Transmission System Operators for Electricity.

A key outcome of the validation activities was that the policies presented, as part of the complete policy landscape presented, were considered applicable and relevant to the CNI industry by the key stakeholders. In addition the terminology remains consistent to that used within the CNI domain. However, it was identified and agreed that facilitated interaction with experts provided a more suitable platform for communicating the key concepts. In summary, any toolkit will be of limited use unless the academic & industry experts behind the models are present to facilitate and provide interpretation of the complex concepts.

The report then moves on to highlight the key policy outcomes in more detail for all the work in the CNI case study in the third year of the project. For example:

- It was generally accepted that a CNI Operator is better placed, and thus more effective, at mitigating security risks directly rather than through following rules defined by a regulator.
- The effectiveness of a rules-based regulatory structure is dependent on how informed the regulator (rules-setter) is of the security of key assets.

There are a number of significant policy insights presented which have been fed into a number of separate policy papers focused on the CNI case study, principally the paper titled 'Economic Impacts of Rules-based vs Risk-based Cybersecurity Regulations in Critical Infrastructure Providers (Bulk Electricity Providers)' which can be found in Appendix E. Also, the CNI case study's KPI assessment is presented in detail in Appendix A.

1. Introduction

This report is the Evaluation tools for providers and policy paper on future and emerging threats of the Critical National Infrastructure (CNI) case study, provided by National Grid. It builds upon the earlier work undertaken in Work Package (WP) 2 covering the case study directly, WP6 covering the economic and system models that are relevant to the CNI case study, WP4 covering the comparative analysis of society's and citizens' views and WP8 which covers the tool support.

1.1 Scope of report

WP2 focuses on the different aspects of security within CNI including policy, regulation, risk assessing and best practices.

The deliverables within WP2 are listed below:

D2.1	Ethical opinion/authorization
D2.2	National Grid Requirements first version
D2.3	National Grid Requirements final version
D2.4	Model Validation
D2.5	Evaluation tools for providers and policy paper on future and emerging threats.

This document is Deliverable 2.5 (D2.5) of WP2. This report presents an overview of the CNI case study tool validation and the validation of the exploitation model of the overall CNI toolkit. In addition, this report presents some of the policy insights from the various validation activities and SECONOMICS summit.

1.2 Overview of the document

This document is organised as follows:

- Section 2 describes the activities to support the design of the toolkit specifically in Year 3 of the project. Also, a clear definition and scope of the toolkit is given to provide context to all the work in this part of the project.
- Section 3 defines the SECONOMICS practice for exploitation of science-based policy models in general but moves toward focussing on how the CNI toolkit will be exploited.
- Section 4 then presents in detail the validation activities to validate the SECONOMICS practice for exploitation specifically in the CNI case study. Following this the results of the validation are presented against the three main SECONOMICS outcomes.
- Section 5 presents some of the key policy insights that have come from the CNI case study part of the project. The policy insights come from three areas which are: the validation activities, SECONOMICS summit and from pan-European coordination.
- Section 6 ends the report with a forward looking perspective on future and emergent threats and how this affects the CNI toolkit but also how the current toolkit takes this into account.

- Appendix A presents the SECONOMICS Key Performance Indicators (KPIs) and how the work of the CNI case study has met those KPIs.
- Appendix B and C presents details of support to toolkit design and validation meetings respectively.
- Appendix D presents the validation results of the CNI case study in detail.
- Appendix E presents the main policy paper on future and emerging threats in CNI titled ‘Economic Impacts of Rules-based vs Risk-based Cybersecurity Regulations in Critical Infrastructure Providers (Bulk Electricity Providers)’.

2. Support to Toolkit Design

Deliverable D2.4, Model Validation, provides motivation for the modelling work by first discussing the advantages and disadvantages of the different regulatory schemes. Through looking at this more analytically two key research questions were generated that the modelling work is based on. These questions are below:

1) Question 1: Which type of regulatory structure would best incentivise and equip CNI operators to be information and cyber secure?
2) Question 2: What are the different societal views of the information and cyber security of CNI and its operators?

These research questions are looked at in completely different ways. To attempt to answer Question 1, measuring the effectiveness of a regulatory system/structure on a CNI operator, a number of economics/mathematical models have been developed that look at this problem from slightly different view points in collaboration with WP6 and WP8. These models are:

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

Both models internalise the regulatory structure that is in place and how the CNI operator reacts to it and other events such as ‘shocks’ or cyber security attacks.

Question 2 is very different to Question 1 as it looks at the sociological aspects of security in CNI. Deliverable D2.4 discussed how we would use the methodologies and techniques of WP4 to perform a comparative analysis on the different views (societal and expert) of the Stuxnet malware utilising different media sources from different countries.

2.1 Developing a Tool for the CNI Case Study

The case of information/cyber security in CNI differs from the other case studies within the SECONOMICS project. Unlike in the case of urban public transport and air traffic management and airports, the end user is not an individual citizen but the distribution networks and other major stakeholders. Even though CNI concern citizens profoundly, it is indirect and the role of CNI is often difficult to comprehend for citizens and society in general.

As a result of this, the tool development of the CNI workstream has been focused around the economic and systems models used to investigate Question 1 above. The purpose of the tool is to provide a visual aid of the models and their outcomes to CNI Operators, Policy Makers and other stakeholders.

The economic and systems models mentioned above were first presented in WP6 deliverable D6.1, ‘A general systems model architecture’, as generic models that had potential to be applied in the security regulation arena. To accurately apply these models to the specific case of the Electricity Transmission Network, a process of model building has been followed which included the analysis, calibration, validation and refinement of the models, as described in D2.4. Given the difficulty of answering the key question (Question 1) analytically the process of validation and refinement with stakeholder involvement has been challenging and became an iterative process that overlapped with the tool building and validation. Nevertheless, this process has been positive overall in producing a more effective model with more informative tools. Technical details about the bespoke models for the CNI case study are presented in deliverable D6.2, 'A report on the interaction of systems models and models of economics, law and society'.

2.2 Toolkit Development and Validation Preparation

In order to exploit the CNI case study modelling work, as described above, a tool has been developed. Rather than referring to a tool we refer to a toolkit which includes a number of components:

1) Underlying Models: mathematical models described above and in D2.4 coded to accept certain user input
2) Infographics: Graphics to front the models but also ensure the context to the CNI case study
3) User Interface and Input: A user interface imbedded within the infographics for the stakeholders to use.

Deliverable D2.4 discussed the underlying models validation and refinement in significant detail. Here we present the different meetings and workshops that took place between the SECONOMICS partners regarding the infographics, user interface design and evaluation and how they provided support to technical testing of the toolkit. Also, it was essential to prepare for the validation of the toolkit with the stakeholder panel.

These are detailed in the table below.

Date	Attendees	Workshop / Meetings Purpose
27th March 2014 **Trento, Italy**	NGRID Security Research Manager, UNIABDN, UDUR, UNITN & ISST	Planning for WP2 toolkit validation and defining of the Seconomics practice of exploitation
22nd - 24th April 2014 **Durham, UK**	NGRID Security Research Manager, UNIABDN & UDUR	Workshop on the outcomes of the Validation of the models and preliminary discussions of what the tool for WP2 can achieve and what it should look like.
27th - 28th May 2014 **Durham, UK**	NGRID Security Research Manager, UNIABDN & UDUR	Workshop to finalise the organisation of the National Grid Validation event in late May covering the models and initial toolkit exploitation validation.
10th - 11th July 2014 **Aberdeen, UK**	NGRID Security Research Manager, UNIABDN & UDUR	Workshop to finalise the preparation of the meeting with DECC to cover Confidence Building and Stakeholder buy-in.
22nd - 24th July 2014 **Durham, UK**	NGRID Security Research Manager, UNIABDN, UDUR, UNITN & ISST	This workshop was to perform the implementation of the tool design, tool calibration and preparation of the next stages of the toolkit exploitation validation.
24th - 27th September 2014 **Trento, Italy**	NGRID Security Research Manager, UNIABDN, UDUR & UNITN	The purpose of the workshop was to analyse the initial validation of the tool and refine the tool design/implementation in preparation for the future validation meetings and the

		SECONOMICS Summit.
13th, 20th & 21st October Teleconferences	NGRID Security Research Manager, UDUR, UNITN & ISST	These calls were to go through specific aspects of the tool design, infographics and GUI for the CNI case study. This included the toolkit preparation for the final validation meetings.
3rd November 2014 Wokingham, UK	NGRID, UNIABDN & UDUR	This workshop was to define and develop the 'What-If' scenarios in preparation of the final part of exploitation model validation.
21st November 2014 Aberdeen, UK	NGRID, UNIABDN & UDUR	This workshop was to further develop the use cases and scenarios in preparation for the ENTSO-E CSP and Cyber group meetings as part of the 'What-If' scenarios (final part of exploitation model validation).
10th December 2014 London, UK	Workshop between NGRID, ISST, UNIABDN & UDUR.	This workshop was to refine the toolkit infographics and user interface to maximise the effectiveness of the exploitation model validation.

Table 1 – Information Workshops and meetings

3. SECONOMICS Practice for Exploitation of Science-Based Policy Models

In this section we discuss how the toolkit will be utilised by our key stakeholders and others to aid policy makers in identifying and designing information and cyber security policy for CNI industries. Through our extensive validation work, we have identified a process by which the stakeholders will use the toolkit, referred to as the ***Exploitation Model***, which is described below:

- **Stakeholder buy-in:** In the first step the user of the toolkit will need to introduce the toolkit to the stakeholder. In order to get their initial buy-in the aim, functionality and background of the toolkit and the underlying models will need to be presented.
- **Confidence Building:** Gaining the buy-in of stakeholders is not done in 'one-hit'. Instead, through the experience of validation (that is discussed in the next section) getting the buy-in of the stakeholders and building their confidence in the toolkit takes multiple meetings.
- **Calibration:** Once the stakeholders have buy-in and confidence in the toolkit, the toolkit needs to be calibrated towards the industry or scenario where information or cyber security policy is being considered. This will include discussions with the stakeholders of parameters to calibrate the models within the toolkit to the particular scenarios the policy maker is interested in. Also, identification of the parameters under the control of the policy maker and the ones defined by the environment. This is done in collaboration with the stakeholders through the discussing of different situations and use cases. This will also further increase the stakeholders' confidence in the toolkit.
- **What-If Scenarios:** With the stakeholders having confidence in the toolkit and collaborated in the calibration of the underlying models, the toolkit can now be presented back to the stakeholders. Specifically, the analysis of use cases and scenarios should be presented to identify outcomes of possible policy decisions.

At this stage we have not identified who we expect to be the presenter of the toolkit and the stakeholders being presented to. The aim is that the presenter is the CNI Operator or Civil Servants and the stakeholders are the head policy makers. However, to validate this Exploitation Model we, as researchers, presented the toolkit to our identified stakeholder panel members and the results of this are discussed in the next section.

4. Validation of Toolkit Exploitation Model

In this section we present the validation activities and results of the toolkit for the CNI case study. We present the activities conducted to validate the Exploitation Model as described in Section 3. Following this we summarise the results of the validation against the three key SECONOMICS outcomes: User Acceptability, Domain Suitability and Technical Usability.

4.1 Validation Activities

Below we present the validation activities that have been conducted around the CNI case study models and toolkit as a whole. The activities are organised into the four stages of the Exploitation model which were introduction in Section 3 namely:

- Stakeholder Buy-in
- Confidence Building
- Calibration
- What-if Scenarios.

In order to provide a complete picture of the validation of the Exploitation Model the validation meetings/workshops that were discussed in detail in deliverable D2.4 are also presented here.

4.1.1 Stakeholder Buy-in

This first stage of the exploitation model was performed (and validated) mostly in the second Year of the SECONOMICS project through engagement with the members of the CNI Stakeholder Panel. These stakeholders are National Grid's Digital Risk & Security team, the UK's Centre for the Protection of National Infrastructure (CPNI) and the European Network of Transmission System Operators for Electricity (ENTSO-E). Detailed description of the stakeholders and their relevance to the CNI case study are given in earlier deliverables of this work package (D2.3, D2.4) and also in deliverable D9.8, First Stakeholders Panel report.

In the table below we present the different meetings that took place to gain the initial stakeholder buy-in across our key stakeholders.

Date	Workshop / Meeting	Detail
31st January 2013	SCADA and Control Systems Information Exchange (SCSIE) - Run by CPNI	The SCSIE is a meeting that brings together CNI operators within the UK and is run by the CPNI. A presentation was given on the SECONOMICS project with a focus on the CNI case study and the research into different regulatory structures. This meeting was the first opportunity to present SECONOMICS CNI workstream to CPNI to gain their buy-in into the project.
3rd April 2013	ENTSO-E Cyber Group meeting	This group brings together security professionals from the various Electricity Transmission System Operators across Europe with a particular focus on cyber security. A high level presentation was given on deliverable D2.3 and the aims of the CNI case study and a view of what the modelling work was hoping to achieve and how this could

		benefit the members of ENTSO-E when dealing with their national regulators. This meeting was the first opportunity to present SECONOMICS CNI workstream to the ENTSO-E Cyber group to gain their buy-in into the project.
26th November 2013	NGRID Validation meeting 1	National Grid Validation Meeting 1 with the DR&S Leadership. Focusing on introducing and explaining the Subsidy & Incentives (Agility) model, Stuxnet media analysis and partially on the Policy Coordination (Sustainability & Resilience) model. Details of the meeting and attendees are provided in deliverable D2.4.

Table 2 – Meetings & Validation Events to gain stakeholder buy-in

4.1.2 Confidence Building

As explained in Section 3, gaining stakeholder buy-in does not simply take one meeting but multiple iterations. In the CNI case study, we found that the stakeholders were keenly interested in the scientific background to the economic models being used and how they were being honed to the CNI space. This included detailed discussions on the model aims, generic scientific background, specific application to CNI and how the models could potentially be used.

In the table below we present the different meetings that took place to cement the stakeholder buy-in to build confidence in the models and by implication the toolkit. We also took the approach to expand our key stakeholder base in the government space to maximise the impact of the results further into the project. We initially focused on engaging with CPNI as they are a pan-government agency in the UK. However, we engineered an opportunity to discuss SECONOMICS and the CNI case study work with the lead government department for energy regulation, Department of Energy and Climate Change (DECC) and also the UK Cabinet Office who drive regulation at the top level of government which then filters down to the lead departments such as DECC. More details about DECC and UK Cabinet Office can be found in deliverable D2.3.

Date	Workshop / Meeting	Detail
27th January 2014	NGRID Validation Meeting 2	National Grid Validation Meeting 2 with the DR&S Leadership. Focusing on providing further technical/scientific detail about the Policy Coordination (Sustainability & Resilience) model and partially on the Subsity & Incentives (Agility) model. Details of the meeting and attendees are provided in deliverable D2.4.
7th May 2014	CPNI Meeting 3	Validation Meeting 3 with the CPNI. Specifically in attendance were the CNI Security Advisors from CPNI who cover the energy and utilities space. Focusing on the background and context of the CNI case study as well as both economic models at a high level. Details of the meeting and attendees are provided in Appendix C.
3rd June 2014	ENTSO-E Cyber Group Meeting 5	ENTSO-E Cyber group Meeting 5. In attendance were the cyber security professionals from the Electricity Transmission Operators across Europe. Having introduced SECONOMICS and the CNI case study at a previous meeting, here we focused on introducing and explaining in more detail the Subsidy & Incentives (Agility) model and the Policy Coordination (Sustainability &

		Resilience) model. Details of the meeting and attendees are provided in Appendix C.
15th July 2014	UK Cabinet Office Meeting 6	UK Cabinet Office Meeting 6. In attendance were Cabinet Office advisors on the National Cyber Security Programme for the lead government departments. They have a keen interest in understanding the effects of different types of regulation on the security within CNI organisations. Presentation and the discussion focused on the background and context of the CNI case study as well as the Policy Coordination (Sustainability & Resilience) and Subsidy & Incentives (Agility) models at a high level. Details of the meeting and attendees are provided in Appendix C.
22nd July 2014	DECC Meeting 7	Meeting 7 with DECC, the lead government department in the UK for energy. Specifically in attendance were the head and members of the Energy Resilience Cyber team responsible for managing CNI Cyber risks within the energy industries in the UK. Presentation and the discussion focused on the background and context of the CNI case study as well as the the Policy Coordination (Sustainability & Resilience) and Subsidy & Incentives (Agility) models at a high level. Details of the meeting and attendees are provided in Appendix C.

Table 3 – Meetings & Validation Events for confidence building

4.1.3 Calibration

Once the key stakeholders have bought into the models and toolkit, they need to be calibrated to accurately describe the landscape of security regulation and how the CNI operator acts and reacts within that. Calibration requires the input of the security subject matter experts within the key stakeholders which in this case are National Grid's DR&S leadership and the members of the ENTSO-E Cyber group. To that end the validation meetings to perform the calibration focussed on these stakeholders as described in the table below.

Date	Workshop / Meeting	Detail
29th May 2014	NGRID Validation Meeting 4	Validation Meeting 4 with the DR&S Leadership. This meeting focussed on calibrating the parameters of the Subsidy & Incentives (Agility) model part of the toolkit. In particular: • the game-theoretic process by which the model operates was discussed and agreed, • Parameter choices of the actors (policy maker, firm and attacker) were described in detail and agreed • The model parameters that describe the key trade-offs were discussed is great detail so that could be set to accurately describe the landscape • Sample outputs of the model were present to set expectations and get feedback as to how they could be used by the CNI Operator and policy makers. Details of the meeting and attendees are provided in Appendix C.
11th August 2014	NGRID Validation Meeting 8	Validation Meeting 8 with the DR&S Leadership. The key focus of this meeting was to complete the calibration of the Policy Coordination (Sustainability & Resilience) model

		part of the toolkit, which is described here, and to present some initial outcomes of the toolkit, which is discussed in Table 5 the next subsection. The following calibration areas were discussed that are relevant to the Policy Coordination model: • The sets of parameters around the directed regulated (CNI) assets and the non-core (corporate assets) • Diminishing marginal returns to security investment theory and reality • The assumed attack dynamics including risk levels and payoffs • CNI Operator's time preferences and discount rates. Details of the meeting and attendees are provided in Appendix C.
18th September 2014	ENTSO-E Cyber Group Meeting 9	ENTSO-E Cyber group Meeting 9. In attendance were the cyber security professionals from the Electricity Transmission Operators across Europe. Building on the stakeholder buy-in built up in previous meetings, this meeting focused on calibration. Specifically the Policy Coordination (Sustainability & Resilience) model and gaining further insight and agreement on the calibration areas discussed in the NGRID Validation Meeting 8 above. Details of the meeting and attendees are provided in Appendix C.

Table 4 – Meetings & Validation Events for calibration

4.1.4 What-If Scenarios

With the models now calibrated the use cases and scenarios can be presented back to the key stakeholder using the toolkit. As the models in this case study focus on public policy the key stakeholders who could use the outcomes are CNI Operators and Policy Makers. Therefore, in the first instance the toolkit was presented to NGRID and ENTSO-E. The table below describes these meetings in more detail.

Date	Workshop / Meeting	Detail
11th August 2014	NGRID Validation Meeting 8	Validation Meeting 8 with the DR&S Leadership. Here we discuss the scenario presentation part of the meeting. Following the calibration of parameters, tradeoffs and assumptions, the key scenario of a 'Rules-based regulatory regime for TSOs across Europe' was presented. In addition, outcomes of the regulation being in place were presented where the artifical regulator has different levels of information about the CNI Operator's assets. Details of the meeting and attendees are provided in Appendix C.
10th November 2014	NGRID Validation Meeting 10	Validation Meeting 10 with the DR&S Leadership. In this meeting a number of use cases and scenarios of the Subsidy & Incentives (Agility) model were presented. In particular: • Levels of payoff to the policy maker across the phase space dependent on their need of assurance • Changes to the phase space as the potential levels of unindemnified damage vary • Policy makers difficulty in aiming for a mixed rules

		and risk based response from the CNI Operator. Details of the meeting and attendees are provided in Appendix C.
2nd December 2014	ENTSO-E CSP Meeting 11	ENTSO-E Critical Systems Protection group Meeting 11. In attendance were the overarching security leads from the Electricity Transmission Operators across Europe. These member representatives work closely with the Cyber group representatives. Therefore, we were able to build on the stakeholder buy-in built up in previous ENTSO-E Cyber group meetings to discuss where to work with SECONOMICS had reached and some initial outcomes, particularly around the Subsity & Incentives (Agility) model. Details of the meeting and attendees are provided in Appendix C.
3rd December 2014	ENTSO-E Cyber Group Meeting 12	ENTSO-E Cyber group Meeting 12. In attendance were the cyber security professionals from the Electricity Transmission Operators across Europe. Building on the stakeholder buy-in built up in previous meetings, this meeting focused on presenting scenarios built up from the Policy Coordination (Sustainability & Resilience) model and detailed usecases/scenarios related to the phase diagram of the Subsidy & Incentives (Agility) model. Details of the meeting and attendees are provided in Appendix C.

Table 5 – Meetings & Validation Events for 'What-if' scenarios

4.2 Validation Results

In deliverable D2.4 we discussed the validation of the models in detail. Here we will be looking at the validation of the tool as well as the further refinement of the models that the tool is based on. Specifically, when we discuss validation we are referring to the validation criteria that was determined early on in the Seconomics project and documented in deliverable D7.1, Validation Plan. This deliverable documented the validation criteria for the three industry case studies against the headline SECONOMICS outcomes: User Acceptability, Domain Suitability and Technical Usability. Here we present a summary of the validation results against each of these. More detail results can be found in Appendix D and in deliverable D8.5, 'Consolidated Validation and Evaluation of Toolkit'.

4.2.1 User Acceptability

The CNI case study models were built upon clear general models, accepted by the academic community. The detailed models were accepted by all the key stakeholders and further meetings led to valuable and robust feedback being received and iterative changes being implemented appropriately.

Stakeholders gave high praise in regards to how the complex concepts had been portrayed. Feedback indicated the chosen approach visually presented the results in a clear, concise and useful manner.

The tool was carefully considered and evaluated by the members of the stakeholder panel. A multi-view perspective was achieved with explicit linkages identified and implemented appropriately with relevant stakeholder input. The tool was identified as being easy to use however research indicates the limited application of evaluation tools in this context. This is due to the complexity and qualitative nature of understanding how CNI Operators respond to security regulation as demonstrated by the volatility/ unpredictability of scenarios.

4.2.2 Domain Suitability

The CNI case study models are built upon detailed and appropriate information in deliverable D2.3 that include examples of relevant scenarios in CNI. Further evidence was elicited from meetings between UNIABDN, UDUR and NGRID. The models inherently integrate the security, economic and social perspectives of CNI.

Involvement with key stakeholders, CPNI, DR&S leadership and ENTSO-E cyber group, led to useful feedback and culminated in an agreement being reached regarding the high level domain suitability achieved by the models.

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

4.2.3 Technically Usability

After numerous validation meetings, with key stakeholders including ENTSO-E, CPNI and the DR&S leadership team, results indicated a variety of beneficial results and outcomes. It was further agreed upon as to how the process and information generated could be turned into policy and regulatory recommendations to meet the aims of WP2 and SECONOMICS.

Very positive feedback was given as to the importance and quality of the technical academic rigour demonstrated by the models. The manner by which it was displayed was identified as being both clear and useable.

However, it was identified and agreed that facilitated interaction with experts provided a more suitable platform for communicating the key concepts. In summary, any toolkit will be of limited use unless the academic & industry experts behind the models are present to facilitate and provide interpretation of the complex concepts.

5. Policy Insights from Validation

5.1 Summary of Findings from the Validation

The validation results focus on how well the toolkit, as a whole, shows that the Exploitation Model works for the underlying scientific background, models and graphical user interface. In this section, however, we present a summary of the policy findings that have come out of all the scientific work and validation meetings/workshops. The wider understanding and analysis of policy in the area of CNI security is much larger than can be put in this section. Instead more detail can be found in a policy paper which is introduced in Appendix E.

Summary findings:

- It was generally accepted that a CNI Operator is better placed, and thus more effective, at mitigating security risks directly rather than through following rules defined by a regulator. However, there was a strong view that through achieving compliance to a set of defined rules, there was a level of corporate accomplishment that security is being handled appropriately. This suggests some complacency and false sense of security where a rules-based regulatory regime is implemented.
- The effectiveness of a rules-based regulatory structure is dependent on how informed the regulator (rules-setter) is of the security of key or core assets. With IT architecture differing across each and every organisation it will be difficult for a regulator to identify which are a CNI Operators core assets accurately. Therefore, developing a rule set for core assets that will achieve the level of security that the regulator is happy with will be a challenge as some CNI operators may exploit gaps in the regulation that will effectively move assets for the core to non-core asset classes.
- A regulator’s payoff is acutely dependent on what it values as important, hence the notion of utility described earlier. If a regulator values assurance i.e. demonstration of compliance to security rules, their payoff will be higher the more stringent the rules are. However, if they value the limiting or the absence of security incidents affecting the service provided by the CNI Operator then there is only a small increment in the regulators payoff as the security rules become more rigid. Therefore, understanding what the regulator or policy maker values from their CNI operators is key to understanding the balance between rules-based and risk-based regulation.
- Cultural attitudes vary widely in different jurisdictions and this can have a significant impact on how firms and CNI Operators react to security regulation, or the lack of it. In some jurisdictions where there is a risk-based regulatory system for security, CNI Operators respond in a collaborative manner with the regulator and government agencies to develop a security posture that all buy into. However, there are other countries where CNI Operators and firms in general choose to do very little in security with similar risk-based regulations in place. This is causing regulators to re-think in such countries, particularly in the EU.

- Developing a mixed response from the regulator including both rules-based and risk-based seems difficult given how the budget constraint cuts that region on the policy phase diagram. However, the view of many security leaders involved in this work is that a mixed regulatory response could be implemented. Specifically, rules could apply to CNI Operators that were less security mature and for those CNI Operators above a certain maturity threshold (i.e. those with an established risk management and mitigation framework) a risk-based regulatory framework could apply. In this way, the rules-based regulation would bring up those organisations below the bar and the risk-based regulation would allow the mature organisations to be innovative and lead the industry in security. Of course, identifying the maturity threshold is not a simple question and, as shown above, levels of risk aversion/acceptance may differ between firms and a policy maker.
- Due to the lack of cyber attacks in CNI with direct impact on the services provided, such as energy delivery, a data-driven approach to designing security regulation in this space would be ill-conceived.

5.2 Summary of Findings from the SECONOMICS summit

At the SECONOMICS Summit a designated panel was scheduled focussed solely on the CNI workstream with the aim being to contextualise the risk-based vs rules-based question in security regulation. The organisation of the panel is described in the following table:

No.	Time slot	Presenter	Workshop / Meetings
1	20 mins	NGRID SECONOMICS Partner	Context presentation about the CNI case study in SECONOMICS. Including an introduction of the Risk vs. Rules regulatory questions in Cyber Security. Also an introduction of the panellists and organisations they represent.
2	20 mins	Chair of the ENTSO-E Cyber Group	Presentation on the cyber security and critical ssets protection of core CNI from the point of view of the Chair of the ENTSO-E Cyber group, representing all the TSOs across Europe.
3	15 mins	All	Plenary Q&A Session Introduced by UK Cabinet Office through a commentary on the previous presentation
4	20 mins	CPNI Cyber Security Advisor	Presentation on encouraging the UK Oil and Natural Gas (ONG) sector to secure their critical systems.
5	15 mins	All	Plenary Q&A Session Introduced by UK Cabinet Office through a commentary on the previous presentation

Table 6 – Meetings & Validation Events for 'What-if' scenarios

After providing context to electricity transmission, CNI security and the regulatory environment in agenda item 1, the Chair of the ENTSO-E Cyber group presented on the 'Increasing complexity of the IT components in operational technology'. This presentation focussed on the current vulnerabilities and threats in the CNI space of Operational Technology (OT) and how it is expected they will evolve in the future. In the first Plenary Q&A session the following was discussed:

- Government/regulators forcing diversity when procuring key OT/SCADA to reduce vulnerabilities and potential threats materialising. The difficulties around doing

this and the limitations government has to push businesses towards certain decisions.
- Creating a good communicative atmosphere between CNI Operators and government is useful during procurement and key activities. However, governments and regulators lack business awareness.

In agenda item 4 a CPNI Security Advisor gave a presentation on 'The effectiveness and take up of the guidance offered by governments technical and cyber advisory bodies in a risk-based environment'. A Plenary Q&A session followed and the discussion included the following points:

- Whether a regulator in a risk-based environment should take a more proactive role in regulating the sector. Views of the panel were that having regulation may make companies less willing to co-operate but that it is important that fully informed policy making occurs – whichever approach is adopted.
- Smaller stakeholders could be a security weak link in the chain and how should a risk mature company/regulator deal with a key smaller stakeholder from a cyber-perspective? Views from the panel were that connections with these companies should be identified and they should be incentivised to communicate and co-operate with government. Also through the government offering of free-to-use security frameworks could increase the overall security posture of smaller companies that supply to CNI Operators.

5.3 Pan-European Co-ordination

One of the stakeholder panel members for the CNI case study, European Network of Transmission System Operators for Electricity (ENTSO-E), has provided us an excellent opportunity to engage with key stakeholders across Europe. Details of the meetings, activities and discussions are given in section 4. There has been much engagement with the ENTSO-E Critical Systems Protection group and Cyber group across many meetings over the last two years which are present in the earlier section. Therefore, rather than discussing further our engagement with ENTSO-E, we focus here instead on our other European engagement relevant to the CNI case study.

European Commission's Preliminary Workshop comparing U.S. Cybersecurity framework and EU NIS Platform approaches.

This workshop provided an opportunity to discuss and talk credibly in the presence of industry including other CNI operators and the European Commission policy officers particularly from DG-Connect. NGRID was a member on one of the panels at the workshop to discuss risk management frameworks within a corporation. Whilst on the panel NGRID introduced the SECONOMICS project, specifically the CNI case study and how we are tackling the key research questions around risk-based versus rules-based regulation as this has a significant impact on internal risk management. The audience were keenly interested in this topic and any output from the research as this would align well with the possible approaches the European Commission could take in cyber security.

6. Future and Emergent Threats

Future and emerging threats is a theme within the SECONOMICS project that runs through every stage of the CNI case study. In Deliverables D2.2 and D2.3, National Grid Requirements, the focus was to identify and understand National Grid's view of the future and emerging threats to CNI. In D2.4, we presented how NGRID's view of the future and emergent threats fed into the two CNI case study models, Policy Coordination and Subsidy & Incentives models.

Here we add to NGRID's view of the future and emergent threats following the outcome of all the validation meetings, SECONOMICS summit and interviews with members of the CNI case study panel at the summit.

Some specific threats and avenues of concern in the future are highlighted below:

- Predominant threats come from nation states. There are a lot of threats from adversarial nation states potentially taking control of Energy Companies they may want to bring down at some point in the future. Another possible threat is the insider threat. There are also threats from activists and hacktivists.
- Threats can come also from informal procurement. CNI Operators can buy something that is already infected, from a cyber perspective, as there is often a false sense that the vendor has taken the adequate steps to protect their product. However, the product can have exploitable vulnerabilities within it.
- There are threats around the life cycle management. Engineers used to install things (OT equipment) on their own accord for the last 40 years. Now, OT equipment that is being installed within CNI Operators has not got a life cycle and reliable inventories are not being kept. With OT equipment now including a significant amount of IT, there will be unpatched IT assets in the core CNI environment.
- There are an increasing number of viruses and malware out in the wild. Even if they are not targeting the energy sector, they could take out the energy sector because the vulnerabilities they exploit are not sector specific.
- Connectivity - Every company wants more and more data and they are connected to more and more company systems. They are opening more doors than they are closing.

More holistically, we are much more dependent on the internet now, but at the same time this causes the greatest threat. CNI is dependent on the internet as well, not just citizens. All this exposure to the internet is attractive to people who want to exploit it for their own (malicious) purposes. A circle of hacktivists, criminals and, at the other the end of the scale, nation states could have this intention.

7. Conclusion

This report builds on the modelling validation work in Deliverable D2.4, CNI Model validation, and presents in detail the work in the CNI case study in Year 3 of the SECONOMICS project.

The focus of this report was to define and explain the SECONOMICS practice of exploitation of the CNI toolkit and how the four different stages of the practice have been validated. The 12 validation activities with the key members of the CNI stakeholder panel, National Grid's Digital Risk & Security leadership, the UK's Centre for the Protection of National Infrastructure and European Network of Transmission System Operators for Electricity clearly validated the practice of exploitation.

A key outcome of the validation activities was that the policies presented, as part of the complete policy landscape presented, were considered applicable and relevant to the CNI industry by the key stakeholders. In addition the terminology remains consistent to that used within the CNI domain. However, it was identified and agreed that facilitated interaction with experts provided a more suitable platform for communicating the key concepts. In summary, any toolkit will be of limited use unless the academic & industry experts behind the models are present to facilitate and provide interpretation of the complex concepts.

The report then moves on to highlight the key policy outcomes for all the work in the CNI case study in the third year of the project. Particularly, the policy insights from the various validation activities, the CNI panel at the SECONOMICS summit and through pan-European coordination. There are a number of significant policy insights presented which have been fed into the separate policy papers that have been and currently are being produced in the CNI case study. The first of those is presented in Appendix E titled 'Economic Impacts of Rules-based vs Risk-based Cybersecurity Regulations in Critical Infrastructure Providers (Bulk Electricity Providers)' and others included as part of deliverable D6.4, 'A set of policy papers'.

The report then concludes with a forward looking perspective on future and emergent threats and how this affects the CNI toolkit but also how the current toolkit takes these into account.

8. References

1. SECONOMICS D2.2: National Grid Requirements, First Version
2. SECONOMICS D2.3: National Grid Requirements, Final Version
3. SECONOMICS D2.4: National Grid Model Validation
4. SECONOMICS D6.4: A Set of Policy Papers

Appendix A: Assessment of Project KPIs

ID	Short Name	Key Performance Indicator value
1	*METHODOLOGY and GUIDELINES for POLICY MAKERS* *[Scale 1-5]*	3. **Explicit linkage of produced artefacts:** There is an explicit linkage with the Security and Society Stuxnet media analysis (WP4). 4. **Formal linkage of produced artefacts** There is a formal linkage between the Economic and Systems models of WP6 and the toolkit implemented through WP8. 5. **“Local” Usability of methodology in producing artefacts:** Whilst the Toolkit only requires the stakeholder to have a specific knowledge of the CNI, the toolkit on its own is of limited value to a policy maker. Due to the complexity of CNI security more value is placed upon the interpretation of the model output by industry and academic experts.
2	*MODELLING NOTATIONS and LANGUAGES for SYSTEMS DESCRIPTIONS* *[Scale 1-5]*	2. **Computer Aided support of consistency:** There are computer aided support behind the Security and Society Stuxnet media analysis (WP4) and are tool supported. 4. **Formal characterization of constructs:** The Policy Coordination and Subsidy models of WP6 are clearly constructed mathematically following numerous validation meetings with the key CNI stakeholders. 5. **“Local” Usability of construct:** The constructs and artefacts of the toolkit are self-contained so that they are understandable to any user.
3	*ALGORITHMS and COMPUTATION for ECONOMICS and RISK ASSESSMENT* *[Scale 1-4]*	4. **Formal or operational evidence of efficiency:** The toolkit is standalone and the model computations are fully automatic. Also, the mathematical models in WP6 solve things analytically in the most part thus can provide an exact solution when solving problems. There is formal evidence in the output of the models which shows the efficiency of the models.
4	*TOOL*	The tool supports the methodology and computation so the same criteria apply to the supported artefacts. It is fully integrated with methodology.
5	*USAGE POTENTIAL* *[Scale:* *Applied on the case study 1-4* *Requiring Human Effort 1-3]*	**The toolkit can be applied to a case study:** 2. Results can be understood by the key CNI stakeholder for the Security and Society (WP4) models. 3. However the Policy Coordination and Subsidy models (WP6) cannot be applied in any significance by the stakeholder due to the complex nature of the interactions of CNI security policy on a monopolistic CNI Operator. 4. Not within remit/interest. **Required human effort to apply toolkit to a case study** 2. Equivalent to manual approach for Security and Society (WP4). Major changes will require major remodelling. 3. Saves effort for Policy Coordination and Subsidy (WP6) models.
6	*INNOVATION POTENTIAL* *[Scale 1-4]*	3. The technique can be used by revising the existing processes for Security and Society (WP4) models. 4. The technique can be used without major revision for the Policy Coordination and Subsidy (WP6) models and contributes to refining the existing process.

ID	Short Name	Key Performance Indicator value
7	CASE STUDY REPRESENTATIVENESS [Scale: Detail of Investigation 1-4 Facets considered in the Scenario 1-4]	**Detail of investigation** 2. Empirical exercise with researchers to simulate steps was performed for the Security and Society media analysis of Stuxnet (WP4) with the analysis of national media for the related security aspects. 4. Empirical exercise by stakeholders to simulate a significant proportion of the process. This was the level reached with the Policy Coordination and Subsidy models (WP6), as these models implement as part of the toolkit looks at the entire CNI security policy landscape at a juridicational (national) and European level. **Facets considered in the scenario** 2. Several aspects for a considered scenario applies to the Security and Society (WP4) model particularly awareness, social reliance on CNI and how CNI cyber security is of immense importance 4. Multiple views to multiple aspects applies to the Policy Coordination and Subsidy (WP6) models as they consider the problem of effective CNI security regulation from multiple view at a juridicational (national) and European level.

Appendix B: Detailed list of Support to Toolkit Design Activities

Date	Attendees	Workshop / Meetings Purpose
27th March 2014 Trento, Italy	NGRID Security Research Manager, UNIABDN, UDUR, UNITN & ISST	Planning for WP2 toolkit validation and defining of the Seconomics practice of exploitation
22nd - 24th April 2014 Durham, UK	NGRID Security Research Manager, UNIABDN & UDUR	Workshop on the outcomes of the Validation of the models and preliminary discussions of what the tool for WP2 can achieve and what it should look like.
27th - 28th May 2014 Durham, UK	NGRID Security Research Manager, UNIABDN & UDUR	Workshop to finalise the organisation of the National Grid Validation event in late May covering the models and initial toolkit exploitation validation.
10th - 11th July 2014 Aberdeen, UK	NGRID Security Research Manager, UNIABDN & UDUR	Workshop to finalise the preparation of the meeting with DECC to cover Confidence Building and Stakeholder buy-in.
22nd - 24th July 2014 Durham, UK	NGRID Security Research Manager, UNIABDN, UDUR, UNITN & ISST	This workshop was to perform the implementation of the tool design, tool calibration and preparation of the next stages of the toolkit exploitation validation.
24th - 27th September 2014 Trento, Italy	NGRID Security Research Manager, UNIABDN, UDUR & UNITN	The purpose of the workshop was to analyse the initial validation of the tool and refine the tool design/implementation in preparation for the future validation meetings and the SECONOMICS Summit.
13th, 20th & 21st October Teleconferences	NGRID Security Research Manager, UDUR, UNITN & ISST	These calls were to go through specific aspects of the tool design, infographics and GUI for the CNI case study. This included the toolkit preparation for the final validation meetings.
3rd November 2014 Wokingham, UK	NGRID, UNIABDN & UDUR	This workshop was to define and develop the ‘What-If’ scenarios in preparation of the final part of exploitation model validation.
21st November 2014 Aberdeen, UK	NGRID, UNIABDN & UDUR	This workshop was to further develop the use cases and scenarios in preparation for the ENTSO-E CSP and Cyber group meetings as part of the ‘What-If’ scenarios (final part of exploitation model validation).
10th December 2014	Workshop between NGRID, ISST, UNIABDN &	This workshop was to refine the toolkit infographics and user interface to

London, UK	UDUR.	maximise the effectiveness of the exploitation model validation.

Table 7 – Information Workshops and Meetings

Appendix C: Detailed list of Validation Activities

Meeting 3: CPNI

Date: 7th May 2014 at 15:00

Venue: National Grid Head Quarters, 1-3 Strand, London, UK WC2N 5EH

The following people were in attendance at the Validation meeting with CPNI. Due to national security the names of the representatives from CPNI have not been given but their roles titles have been included in the table below:

Representative	Seconomics Partner Organisation	Role
Raminder Ruprai	NGRID	Security Research Manager
Unspecified	CPNI	Security Advisor for Electricity & Gas
Unspecified	CPNI	Security Advisor for Downstream Oil Gas

Table 8 - Validation Meeting 3 attendees

Meeting 4: National Grid Validation

Date: 29th May 2014 at 13:30

Venue: National Grid Head Quarters, 1-3 Strand, London, UK WC2N 5EH and via videoconference with National Grid Warwick, Warwick Technology Park, Gallows Hill, Warwick, Warwickshire, CV34 6DA.

The following people were in attendance at the National Grid Validation meeting. The majority of attendees are members of the National Grid Digital Risk & Security (DR&S) department and their job titles have also been provided:

Representative	Seconomics Partner Organisation	Role
Raminder Ruprai	NGRID	Security Research Manager
Graham Wright	NGRID	Chief Information Security Officer
Steve Collins	NGRID	Acting Chief Information Security Officer
Chris Keay	NGRID	Head of Security Strategy, Policy & Architecture
Lawrence Russell	NGRID	Head of Business Security
Simon Thornhill	NGRID	Head of Privacy
David Willacy	NGRID	DECC Cyber Security Advisor
Matthew Collinson	UNIABDN	

Table 9 - Validation Meeting 4 attendees

Meeting 5: ENTSO-E Cyber Meeting

Date: 3rd June 2014 at 09:00 to 15:30

Venue: Austrian PowerGrid Offices, Vienna, Austria

Detailed attendee list and minutes were taken by the ENTSO-E Cyber meeting co-ordinator but are confidential to the group and are not presented here.

Meeting 6: UK Cabinet Office

Date: 15th July 2014 at 14:00

Venue: UK Cabinet Office, 70 Whitehall, London SW1A 2AS

The following people were in attendance at the meeting with UK Cabinet Office. The job titles/roles have been provided for the attendees from the National Grid Digital Risk & Security (DR&S) department and UK Cabinet Office.

Representative	Seconomics Partner Organisation	Role
Raminder Ruprai	NGRID	Security Research Manager
Unspecified	UK Cabinet Office	National Cyber Security Programme Advisor
Unspecified	UK Cabinet Office	National Cyber Security Programme Advisor
Unspecified	UK Cabinet Office	Other

Table 10 – Validation Meeting 6 attendees

Meeting 7: DECC

Date: 22nd July 2014 at 10:30

Venue: National Grid Head Quarters, 1-3 Strand, London, UK WC2N 5EH

The following people were in attendance at the Validation meeting with DECC. The job titles/roles have been provided for the attendees from the National Grid Digital Risk & Security (DR&S) department and DECC.

Representative	Seconomics Partner Organisation	Role
Raminder Ruprai	NGRID	Security Research Manager
Graham Wright	NGRID	Chief Information Security Officer
David Pym	UNIABDN	
David Willacy	NGRID	Security Manager
Unspecified	DECC	Head of Energy Resilience - Cyber
Unspecified	DECC	Assistant Head of Energy Resilience - Cyber
Unspecified	DECC	Assistant Head of Energy Resilience - Cyber

Table 11 – Validation Meeting 7 attendees

Meeting 8: National Grid Validation

Date: 11th August 2014 at 15:00

Venue: National Grid Head Quarters, 1-3 Strand, London, UK WC2N 5EH and via videoconference with National Grid Warwick, Warwick Technology Park, Gallows Hill, Warwick, Warwickshire, CV34 6DA.

The following people were in attendance at the National Grid Validation meeting. The majority of attendees are members of the National Grid Digital Risk & Security (DR&S) department and their job titles have also been provided:

Representative	Seconomics Partner Organisation	Role
Raminder Ruprai	NGRID	Security Research Manager
Graham Wright	NGRID	Chief Information Security Officer
Steve Collins	NGRID	Acting Chief Information Security Officer
Simon Thornhill	NGRID	Head of Privacy
David Willacy	NGRID	DECC Cyber Security Advisor
Julian Williams	UDUR	

Table 12 – Validation Meeting 8 attendees

Meeting 9: ENTSO-E Cyber Meeting

Date: 18th September 2014 at 09:00 to 15:30

Venue: ENTSO offices, Brussels, Belgium

Detailed attendee list and minutes were taken by the ENTSO-E Cyber meeting co-ordinator but are confidential to the group and are not presented here.

Meeting 10: National Grid Validation

Date: 10th November 2014 at 15:00 to 17:00

Venue: National Grid Head Quarters, 1-3 Strand, London, UK WC2N 5EH and via video conference with National Grid Warwick, Warwick Technology Park, Gallows Hill, Warwick, Warwickshire, CV34 6DA & 40 Sylvan Road, Waltham, MA 02451, United States.

The following people were in attendance at the National Grid Validation meeting. The majority of attendees are members of the National Grid Digital Risk & Security (DR&S) department and their job titles have also been provided:

Representative	Seconomics Partner Organisation	Role
Raminder Ruprai	NGRID	Security Research Manager
Graham Wright	NGRID	Chief Information Security Officer
David Willacy	NGRID	DECC Cyber Security Advisor
Simon Thornhill	NGRID	Global data Privacy Manager
Scott Baron	NGRID	Director of Governance
Matthew Collinson	UNIABDN	Academic
David Pym	UNIABDN	Academic
Greg Cramer	NGRID	Minutes Taker

Table 13 – Validation Meeting 10 attendees

Meeting 11: ENTSO-E Critical System Protection (CSP) Group Meeting

Date: 2nd December 2014 at 09:00 to 15:30

Venue: Ampiron Offices, Cologne, Germany

Detailed attendee list and minutes were taken by the ENTSO-E CSP meeting co-ordinator but are confidential to the group and are not presented here.

Meeting 12: ENTSO-E Cyber Meeting

Date: 3rd December 2014 at 09:00 to 15:30

Venue: Ampiron Offices, Cologne, Germany

Detailed attendee list and minutes were taken by the ENTSO-E Cyber meeting co-ordinator but are confidential to the group and are not presented here.

Appendix D: Detailed Validation Results

In the table below we present the validation criteria for all of the SECONOMICS outcomes of the CNI case study.

Validation Objectives Seconomics Outcomes	User Acceptability	Domain Suitability	Technical Usability
CNI security scenarios	- Discussions and brainstorming with national and supranational stakeholders - Level of acceptance by stakeholders	- Acceptance with NGRID's business of security scenarios - Appropriate stakeholder perspectives are represented - Agreement of suitability by main national and supranational stakeholders	- Accurate scenarios given available threat information - Usable across the electricity transmission network supranationally
Security risk, socio-economic and system models	- All models are well defined and built upon formal evidence - Models are clear and easy to interpret by the stakeholders - Level of acceptance by regulator principally and other stakeholders	- All models built upon evidence of appropriate examples in the area of CNI - Degree of integration of the security, economic and social perspectives - Agreement of suitability by main national and supranational stakeholders	- Degree of monitoring and control on the key trade-offs - The result of the models are clearly defined and interpretable - All the relevant information is presented in a clear and usable manner
Evaluation tools for providers and policy papers on future and emerging threats and regulatory frameworks.	- Explicit linkage with security scenarios and models produced - Multi-view perspective - Dissemination of the policy results to the relevant stakeholders - Acceptance and agreement by stakeholders	- Policies suitability to the CNI industry and judged successfully by stakeholders -Phraseology and terminology consistent with those used in the CNI domain -Non-expert users can potentially apply the tools and policies within their scopes	- Well defined, non-redundant and clear methodology steps - Technically actionable by stakeholders and others within the industry

Table 14 – CNI Case Study Validation Criteria

With all of the activities in mind (model calibration, model refinement and toolkit exploitation validation meetings), in the table below we present how the validation activities and outcomes have met the validation criteria presented in the table above.

Validation Objectives Seconomics Outcomes	User Acceptability	Domain Suitability	Technical Usability
CNI security scenarios	Through numerous workshops with the DR&S leadership and engagement with CPNI, to investigate security regulation in CNI we need to look at it holistically. Instead the concept of current and future states would be considered and this would	DR&S leadership and CISO led the idea of the current and future states as the scenarios. They were presented to the CPNI at the SCSIE meeting in January 2013 and were received with positive feedback. They were also presented and received	Detailed threat analysis with input from DR&S leadership, CPNI and ENTSO-E subgroups at multiple meeting. Other internal and external threat information was fed into the analysis of the current and future states of electricity transmission in

	help focus all workshops.	positively be the ENTSO-E CIP group in November 2012 and then the CSP group in April 2013.	the UK and was thoroughly detailed in deliverable D2.3.
Security risk, socio-economic and system models	All models were built upon clear general models, accepted by the academic community. The detailed models were accepted by DR&S leadership at the validation meetings. Further meetings, held with the ENTSO-E cyber group, CPNI and the cabinet office, led to valuable and robust feedback being received and iterative changes being implemented appropriately. Stakeholders gave high praise in regards to how the complex concept had been portrayed. Feedback indicated the chosen approach visually presented the results in a clear, concise and useful manner.	The Policy Coordination (sustainability & resilience) model and the Subsidy & Incentives (agility) models are built upon detailed and appropriate information in deliverable D2.3 that include examples of relevant scenarios in CNI. Further evidence was elicited from meetings between UNIABDN, UDUR and NGRID. The models inherently integrate the security, economic and social perspectives. Involvement with key stakeholders, CPNI, DR&S leadership and ENTSO-E cyber group, led to useful feedback and culminated in an agreement being reached regarding the high level domain suitability achieved by the models. These validation meetings were held on several occasions, accommodating the iterative pattern of change that was followed based on the robust feedback received.	After numerous validation meetings, with key stakeholders including ENTSO-E, CPNI and the DR&S leadership team, results indicated a variety of beneficial results and outcomes. The DR&S leadership team, in validation meetings, further evaluated the models and agreed they were both relevant and valid. Similar proceedings were held with CPNI, ENTSO-E and the cabinet office. It was further agreed upon as to how the process and information generated could be turned into policy and regulatory recommendations to meet the aims of WP2 and SECONOMICS. Very positive feedback was given around the importance and quality of the technical academic rigour demonstrated by the models. The manner by which it was displayed was identified as being both clear and useable.
Evaluation tools for providers and policy papers on future and emerging threats and regulatory frameworks.	The tool was carefully considered and evaluated. A multi-view perspective was achieved with explicit linkages identified and implemented appropriately with relevant stakeholder input. The tool was identified as being easy to use however research indicates the limited application of evaluation tools in this context. This is due to the complexity and qualitative nature of understanding how a CNI Operators respond to security regulation as demonstrated by the volatility/ unpredictability of	The policies as part of the complete policy landscape presented were considered applicable and relevant to the CNI industry by key stakeholders. In addition the terminology remains consistent to that used within the CNI domain. That being said, while the tool remains useable by non-expert users, it provides limited scope and application for future stakeholders within the domain. The complexity and qualitative nature of CNI security as demonstrated by the volatility/ unpredictability	The integral part of the toolkit is the underlying model. These models are technically accurate and have been based on robust feedback provided during the various stakeholder validation meetings. The models, with proper facilitation from suitably experienced professionals and academics, should be technically actionable by stakeholders and others within the industry. The technical aspects of the model and overall toolkit were well documented and accepted by relevant stakeholders.

	scenarios. It was identified and agreed that facilitated interaction with experts provided a more suitable platform for communicating the key concepts. In summary, any toolkit will be of limited use unless the academic & industry experts behind the models are present to facilitate and provide interpretation of the complex concepts.	of scenarios require facilitated interaction with experts (both academic and industry). In summary, any toolkit will be of limited use unless an expert academic and a suitably experienced CNI industry professional is present to facilitate and provide interpretation of the complex underlying concepts.	However, as mentioned previously, the qualitative nature of the domain means that it's impractical to create a suitable tool that can consider both the qualitative nature of the domain and also accurately take into consideration the rapidly moving and dynamic nature of the cyber security sector.

Table 15 – CNI Case Study Validation Results

Appendix E: Policy paper

A policy paper on future and emerging threats and security regulation in CNI can be found in an annexed document titled ‘Economic Impacts of Rules-based vs Risk-based Cybersecurity Regulations in Critical Infrastructure Providers (Bulk Electricity Providers)’.