SECONOMICS

D2.4 – Model Validation

R. Ruprai (NGRID), C. Keay (NGRID), M. Collinson (UNIABDN), D. Pym (UNIABDN), J. Williams (UDUR), P. Guasti (ASCR), Z. Mansfeldová (ASCR), A. Tedeschi (DBL)

Pending of approval from the Research Executive Agency - EC

Document Number	D2.4
Document Title	National Grid Model Validation
Version	1.0
Status	Final
Work Package	WP 2
Deliverable Type	Report
Contractual Date of Delivery	30.04.2014
Actual Date of Delivery	30.04.2014
Responsible Unit	NGRID
Contributors	UNIABDN, ASCR, UDUR, DBL, UNITN
Keyword List	CNI, Model Validation
Dissemination level	PU

SECONOMICS Consortium

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

1	UNIVERSITÀ DEGLI STUDI DI TRENTO	Università Degli Studi di Trento (UNITN) 38100 Trento, Italy www.unitn.it	Project Manager: prof. Fabio MASSACCI Fabio.Massacci@unitn.it
2	DEEPBLUE	DEEP BLUE Srl (DBL) 00193 Roma, Italy www.dblue.it	Contact: Alessandra 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	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	17/03/2014	Draft	R. Ruprai (NGRID), M. Collinson (UNIABDN), D. Pym (UNIABDN), J. Williams (UDUR)	Initial full draft with Figure 2 missing and Section 4.2 incomplete.
0.2	21/03/2014	Draft	P. Bamford (NGRID), R. Ruprai (NGRID)	Second draft following internal NGRID review. Figure 2 added. Section 4.2 incomplete.
0.3	07/07/2014	Draft	M. Pellot (TMB), R. Ruprai (NGRID), P. Guasti (ASCR), Z. Mansfeldová (ASCR)	Third draft following review by TMB and other comments by all Seconomics partners. Section 4 subsections complete. Three infographics missing.
0.4	07/04/2014	Draft	E. Chiarani (UNITN)	Quality Check. Minor remarks, appropriate amendments made. Three infographics missing.
0.5	10/04/2014	Draft	W. Shim (UNITN)	Scientific Check. Minor remarks, appropriate amendments made. Three infographics missing.
0.6	16/04/2014	Draft	C. Keay (NGRID), R. Ruprai (NGRID)	Internal NGRID Quality Check. Minor remarks focusing on the Executive Summary and appropriate amendments made. Three infographics missing.
0.7	30/04/2014	Draft	A. Tedeschi (DBL)	Infographics constructed and added.
1.0	30/04/2014	Final	R. Ruprai (NGRID)	Cover page updated. Final version ready for submission

INDEX

Executive summary

This report follows deliverable D2.3, National Grid Requirements, where the background to National Grid's UK Electricity Transmission network, as an example of Critical National Infrastructure (CNI), were presented along with National Grid's view of the Current and Future States of electricity transmission in the UK. The different information and cyber security regulatory structures that National Grid is subject to were also introduced.

In this report we recap the details of those regulatory structures and motivate the key question of Work Package 2 (WP2): Which type of regulatory structure would best incentivise and equip CNI operators to be information and cyber secure?

We answer this question by assessing the effectiveness of the different regulatory structures at incentivising CNI operators to be information and cyber secure. Rather than taking a qualitative approach to assessing the effectiveness of the regulatory structures, the report describes the analytical approaches that are being taken, by harnessing the economic and systems models from Work Package 6 (WP6). The first modelling approach takes a holistic view of the electricity transmission ecosystem and is referred to as the Sustainability and Resilience model. The second approach looks in more detail at the interactions of the CNI operator, in response to different regulatory systems being in place and ongoing information or cyber security attacks, using a game-theoretic approach. This model is referred to as the Agility model. This report demonstrates how these models are being parameterised, calibrated and validated towards security regulation in CNI, to answer the key question and objectives of WP2.

In addition, through collaboration with Work Package 4 (WP4), this report investigates the social aspect to information and cyber security in CNI. As citizens are far less aware of CNI that is relied upon by society, the approach taken was to look at cases where information/cyber security issues in CNI have been noticed and discussed in wide scale media. The specific case taken forward was the Stuxnet incident which was described, in detail, in deliverable D2.3. A media comparative analysis on the different views (societal and expert) of Stuxnet was performed using the methodologies described in deliverables D4.2 and D4.3 and details are provided in this report.

These modelling approaches have been validated and calibrated by National Grid's Digital Risk & Security leadership team in a number of meetings. Whilst this is an iterative process the next steps are, to build upon this validation and calibration at a national level with the Centre for the Protection of National Infrastructure (CPNI) and at a supranational level with the European Network of Transmission System Operators for Electricity (ENTSO-E) Cyber Security Protection and Critical Infrastructure Protection subgroups. The ENTSO-E also provides the forum for pan-European coordination with the Electricity Transmission Service Operators across Europe. These different groups are the key stakeholders for WP2 and form the CNI Stakeholder Panel.

1. Introduction

This report is the Model Validation 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 2.4 (D2.4) of WP2. This report presents an overview of the models and preliminary analysis from the technical work packages, principally WP6 and WP4, that are relevant to the CNI case study. In addition, this report focuses on the validation of these models and analysis by the case study's key stakeholders.

1.2 Overview of the document

This document is organised as follows:

- Section 2 builds upon the requirements and work done in D2.3, National Grid Requirements, and sets out the key questions that the modelling work is set to answer.
- Section 3 describes how the general models in WP6 have been applied to the CNI case study. Some high-level technical information is provided around the two WP6 models that are being taken forward in this case study, but detailed technical views of these models are presented in WP6 deliverables, D6.2 and D6.3. Instead, this section focuses on these models from a case study perspective. In addition, the social science comparative analysis methodologies of WP4 are described here that will help to answer the key question on society's views of CNI.
- Section 4 presents the validation activities that have taken place around the two WP6 models and provides a detail walkthrough of the National Grid's internal validation activity of these models. This includes the model validation and calibration meetings that have taken place and some initial outcomes.
- Section 5 looks at how future and emerging threats will input into the models as well as where the information about such threats have been and will continue to be gathered.

- Section 6 presents how the work in the CNI case study, including the modelling work, is being taken to the national and supranational (European) stages. This covers some of the engagement with stakeholders that has already taken place and the potential next steps around the national and supranational validation activities.

2. Model Scoping

CNI providers are a key example of organisations whose information and cyber security risks have potential impacts, beyond their local organisation, but on citizens and society. WP2 introduced the UK Electricity Transmission Network, owned and operated by National Grid. Specifically Deliverable 2.3 (D2.3), National Grid's Requirements, provided an overview of the security threat and risk landscape to this Electricity Transmission network.

D2.3 showed that the largest potential cyber security impact results when the integrity of the overall Electricity Management System is compromised. Manipulating the data being fed into and from the SCADA system, within the Electricity Management System, has the potential to cause significant power outages across the country or, in the worst case, a national black out. The comprehensive threat assessment also identified the various threat actors that could be motivated to cause such an event. Numerous other threats and risks were presented with the potential to impact the confidentiality and availability of the systems and data within National Grid as a CNI operator.

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

Given the potential security impacts for CNI providers in particular, government has a responsibility on behalf of society to ensure that the providers protect the critical systems and services that are essential to the nation. From a governmental regulator perspective, their key concern is how best to ensure such information and cyber security risks to CNI and their operators are appropriately mitigated. Another way of looking at this problem is as follows: How can the CNI operators be incentivised to identify and mitigate the security risks that have the potential to impact the CNI and beyond?

2.1 Spectrum of Regulatory Structures

There are two mains schools of thought around the different types of regulatory structures that the regulator of CNI could implement. The first is a 'Rules-based' system and the second is a 'Risk/Principles-based' system.

In a Rules-based regulatory system the regulator issues a set of rules, requirements or controls that the regulated entities must adhere to. The rules could have been developed following a risk assessment exercise that the regulator had undertaken. As every organisation is different, the rules have to be written so that they can apply to all entities. Therefore they normally do not include product, vendor or system specific information but instead are more general. There are numerous standards in information security that include well-known security controls which are written at this level of

abstraction including the ISO27000 series and National Institute of Standards and Technology (NIST) standards.

In such a regulatory system an organisation may not be required to identify and mitigate security risks but instead need to show adherence to the controls issued by the regulator. This can be achieved through regular compliance audits administered by an auditor on behalf of the regulator. Therefore, part of an organisation's budget for security will include the costs of preparing for, going through and then learning lessons from the regulatory audits. These costs will have an affect on the amount of resources an organisation can spend on actually implementing and improving their security posture.

In its US CNI operations, National Grid is required to adhere to a Rules-based system for security, run by the North American Electric Reliability Corporation (NERC). NERC is an independent organisation that provides guidelines and standards for electricity transmission operators in North America. It has been granted the legal authority to enforce reliability standards on electricity transmission operators by the Federal Energy Regulatory Commission (FERC). NERC develops reliability standards for system operators in North America and monitors the status of various elements of the power distribution system (including cyber security assets). There are a number of reliability standards that NERC has the responsibility of enforcing. The standard which focuses on information/cyber security as well as the CNI aspects of electricity transmission is the Critical Infrastructure Protection (CIP) reliability standards. More details on the specifics of this regulatory regime are given in Deliverable D2.3 'National Grid Requirements'.

On the other end of the regulatory spectrum are the Principles-based regulatory systems. Principles are designed to be general statements that define a goal or objective of the organisation adhering to the principle. In the case of information or cyber security, the main constituent of a principles-based approach is a risk-based approach. Risk mitigation is therefore built into the principles. The principles are normally written at a high level and as a result can be adhered to in a number of different ways dependent on the type of organisation and its level of security posture. As Principles-based regulatory systems have very high level aims it would be difficult to audit an organisation against those objectives. Hence, the regulator may perform a holistic review of the organisation where information or cyber security is simply one pillar of it.

In the UK, National Grid holds a licence to transmit electricity which is granted by the UK government's Department for Energy and Climate Change (DECC). The headline duty of the transmission licence holder within the Electricity Act of 1989 is stated as follows:

'It shall be the duty of the holder of a licence authorising him to transmit electricity to develop and maintain an efficient, co-ordinated and economical system of electricity transmission…'.

Even though the Electricity Act does not specifically require the transmission licence holder to be "secure" one could argue that not having the relevant information security controls in place could jeopardise the efficient, co-ordinated and economical system of electricity transmission. National Grid is then free to decide how they will ensure they are information and cyber secure.

Figure 1 gives a diagrammatic overview of the different regulators, regulatory regimes and high level requirements that National Grid are required to adhere to in the UK and US.

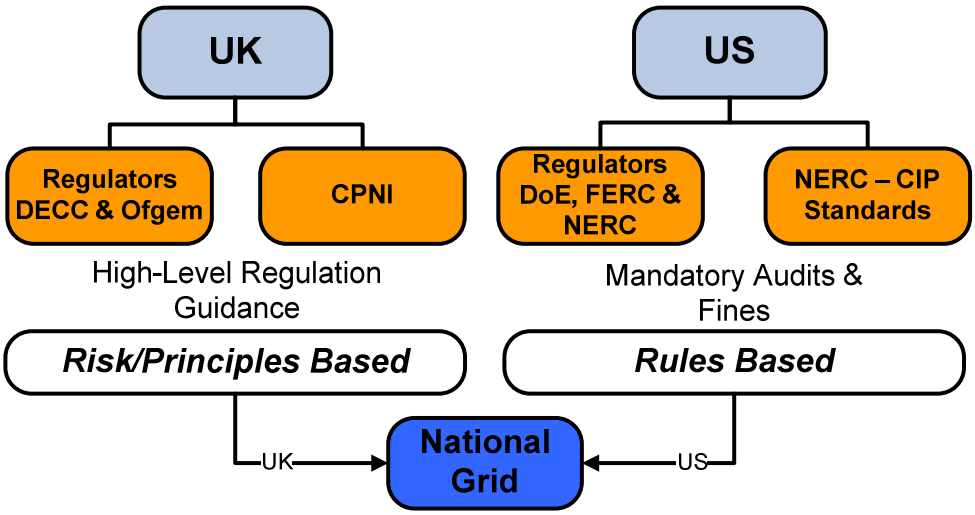


Figure 1 – National Grid Regulation in the US and UK

2.2 Advantages and Disadvantages of Principles-based vs. Rules-based

The UK's Principles-based regulatory system has some key advantages but also some significant disadvantages. The key advantage of this regulatory system is that it gives a CNI operator the flexibility to identify, assess and appropriately mitigate security risks as the organisation sees fit. The conceptual underpinning behind this is that the CNI operator is best placed to understand their infrastructure and thus best placed to understand security risks that affect them. This also allows for CNI operators (in different industries or different parts of the same supply chain) to apply different risk tolerances and controls as they feel appropriate to secure their organisation. If done well, the outcome can be better security buy-in by the organisation as a whole and a more thorough assessment and mitigation of risks for a better overall security posture.

However, there is a directly opposing disadvantage to this. Some organisations may not understand or appreciate the security risks to their business and so may not put a sufficient amount of emphasis on security. Commercial pressures to drive down cost and increase profit are a considerable factor towards this. Historically, this has been the case with many corporate organisations until significant incidents have occurred which have affected or had the potential to affect their organisations. Thus in a nutshell, CNI operators may choose to accept risks they do not fully understand increasing the risk exposure.

In a Rules-based regulatory system there are also advantages and disadvantages. The requirements or rules within such a regulatory structure sets a minimum level of security across all CNI operators, so government, regulators and citizens can be assured that there is a minimum level of security.

A regulatory system that includes detailed rules makes it easier to show and assess compliance against those rules. As a result, regulators can audit CNI operators to assess their compliance against the rules. This can provide the confidence to government and society as a whole that the CNI operators have achieved a certain level of security and provides an opportunity to penalise those organisations that are not meeting the requirements. There is also a view that this negative enforcement can incentivise CNI operators to meet the rules and requirements on an ongoing basis.

However, there are disadvantages to a rules-based regulatory system with a compliance framework. Whilst the rules and requirements, which the CNI operator are required to meet, provides confidence to government and society that there is a minimum level of security, there is no incentive for the organisations to increase their security posture beyond that. In addition, forcing CNI operators to show compliance to the rules means that those organisations are compelled to allocate resources (people and funds) for the auditing process. With limited resources, particularly in information security, this reduces the resources available for implementing security controls that actually mitigate the risks. An additional concern here is that a CNI operator may focus their attention on showing compliance to the rules rather than the actual security risks that are present, potentially leading to a false sense of security.

Also, in such a regulatory system the rules and requirements are devised and set by the regulator, in response to their view of the security risks to the CNI, which could be informed by the CNI operators themselves. Nevertheless there is an inherent delay between the regulator becoming aware of new or changing security risks and then issuing amended rules or requirements as a result. The regulator cannot be as agile in responding to risks to CNI as the CNI operator themselves. Furthermore, there is a higher likelihood that the regulator could have an inaccurate view of the security risks and/or make an incorrect judgement on the rules that mitigate the risks identified. In turn, the CNI operator may be obliged to adhere to rules that are not the most effective in mitigating the risks or, in the worst case, completely redundant.

2.3 Key questions

Above, we have just presented a high-level view of some of the advantages and disadvantages of the main types of regulatory structures that a national government could implement on a CNI operator. The key question that follows from this is: Which type of regulatory structure would best incentivise and equip CNI operators to be information and cyber secure?

We present this problem diagrammatically, in the specific case of National Grid as the UK Electricity Transmission Operator, in Figure 2 below. The information graphic depicts the Electricity Transmission Operator attempting to secure the key components of the CNI against security risks in an environment of vulnerabilities, attackers, exploits and constrained resources with the type of regulation as a key factor.

One could attempt to solve the problem above through a qualitative analysis of the advantages and disadvantages of each regulatory structure using National Grid's UK and US Electricity Transmission networks as a basis. However, formulating any concrete recommendations or outcomes from this would be difficult.

Instead the approach taken to answer this question is to build economic and system models that internalise all the actions of the different parties (government, regulators, CNI operators and attackers) depending on the regulatory structure that is in place. WP6 deliverable D6.1, 'A general systems model architecture', presents some generic economic and system models that could be applied in the security regulation arena.

SECONOMICS - SCENARIO

National Grid Electricity Transmission

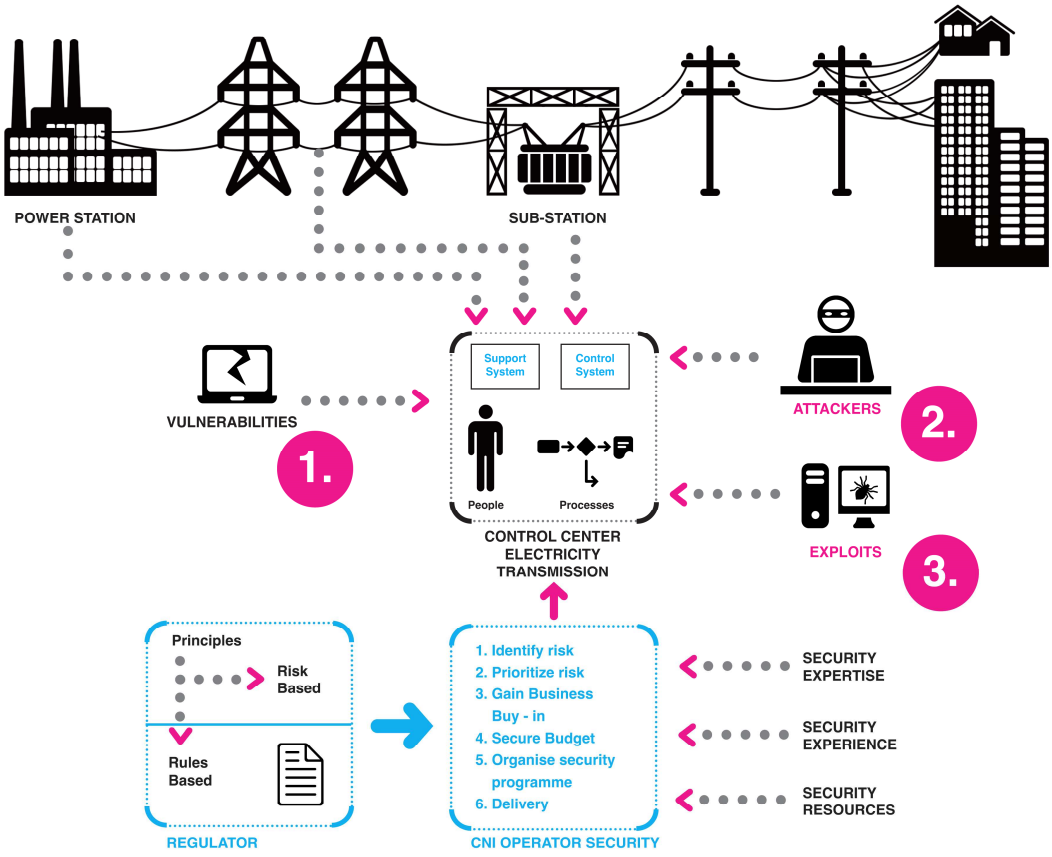


Figure 2 – Infographic: Securing CNI in an environment of vulnerabilities, attackers, exploits, constrained resources and different types of regulatory structures.

WP8 deliverable D8.3, 'Security Problem Modeller', builds upon some of these general models by detailing the:

- model attributes
- intricacies of how the models can be calibrated
- interpretation of the outputs of the models.

In the next section we describe the different economic and system models that have been developed specifically for the CNI setting, which aim to measure the effectiveness of how different regulatory structures incentivise CNI operators to be information and cyber secure.

Another question that is of interest here is: What are the different societal views of the information and cyber security of CNI and its operators? Unlike airports and air traffic

control (WP1) or urban public transportation (WP3), citizens are far less aware of the CNI that is relied upon by society. In addition CNI operators, such as National Grid, do not interact with citizens as consumers of electricity directly so it is difficult to gauge what society's views are of the information and cyber security of CNI and its operators.

WP4 has a focus of studying, analysing and interpreting society's view of security in the different case studies. In particular WP4 deliverable D4.2, 'Report on perception of security and acceptance of risk', looks in detail at the varying social science methodologies at assessing citizen's perception and attitude towards security and risk. The focus of WP4s comparative analysis in the other industry case studies (WP1 and WP3) has been to:

1) Discover the existence of individual and cross-cultural differences in perception of risk and preferences for security measures
2) Focus on the dilemma/tension between privacy and security and between civil rights and acceptance of security measures.

However, these areas are not as relevant when considering the information and cyber security of CNI and its operators as society and citizens do not have a view in the most part. Therefore a different approach needs to be taken to assess this which will be discussed in the next section. We present this problem diagrammatically in the information graphic below.

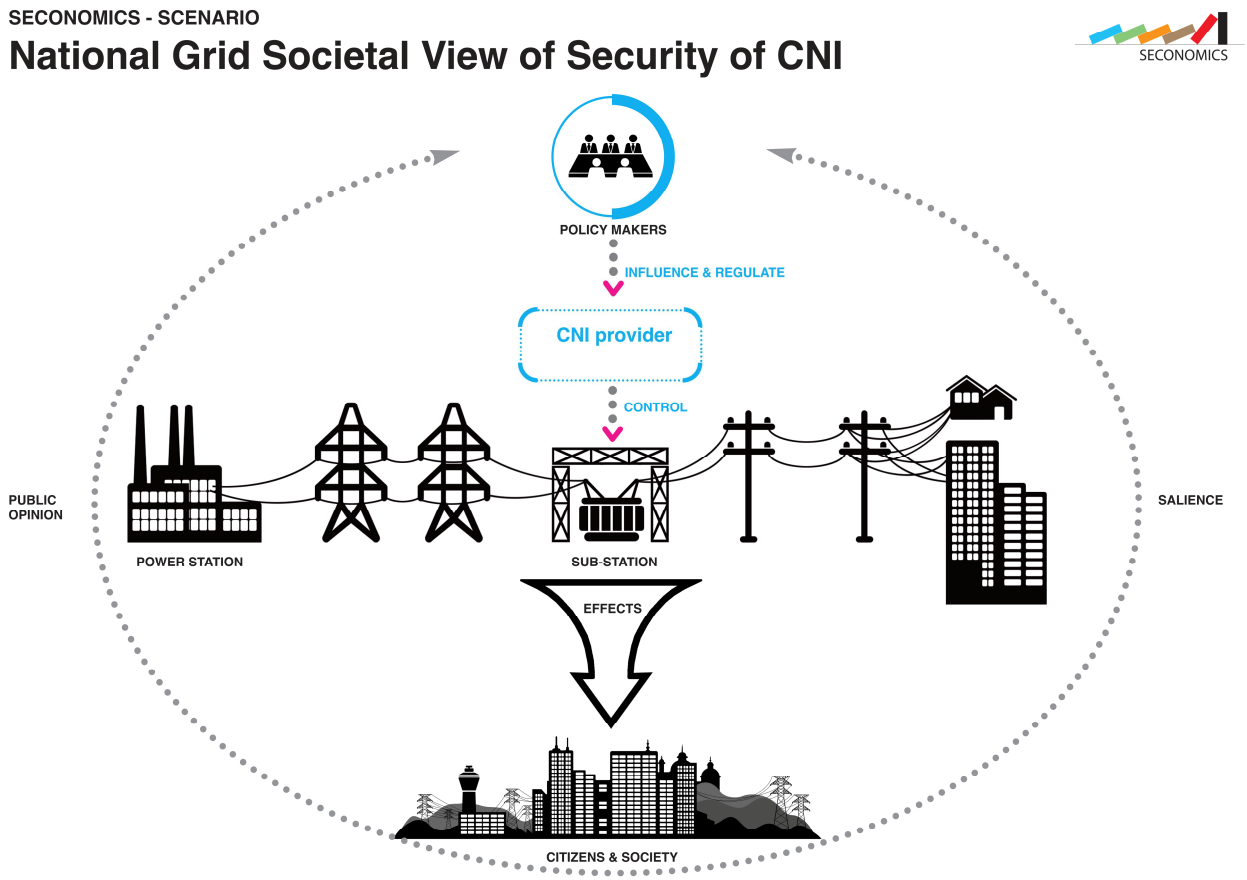


Figure 3 – Infographic: Citizen's & Societal views of information and cyber security in CNI

In the next section we discuss the different modelling approaches and techniques that are being taken to answer they key questions, namely:

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

3. Model Building

This section presents in more detail the different modelling approaches and analysis techniques that are being used to answer the keys questions from the previous section. However, the aim in this particular section is to look at the models from the CNI operator's point of view, in this case National Grid's, rather than the technical point of view which is presented in WP6 and WP4 respectively.

Following this, in Section 3.3 we discuss the numerous meetings and workshops that took place to capture information from the real-world case study to build and calibrate the model.

3.1 Question 1 – Economic & Systems models (WP6)

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

We next look at each model in some detail and describe their different facets in Sections 3.1.1 and 3.1.2 below. Then we bring the models together in one view in Section 3.1.3.

3.1.1 Sustainability & Resilience Model

This model takes a holistic view of the CNI and its operator. It first attempts to measure how well the CNI operator is meeting the 'Normal operating capacity' over time. In the case of National Grid as the UK's Electricity Transmission Operator, the Normal Operating Capacity could be a combined weighted measure of:

- Quality of Transmission
- Security level of the CNI and/or Corporate network
- How close the organisation's CNI network is/has been to a security breach
- Financial loss due to security breaches e.g. direct losses, penalties or fines.

This is the notion of Sustainability of the ecosystem as detailed in deliverable D8.3 and Resilience in Information Stewardship[1]. Figure 4 shows the general idea of sustainability of an ecosystem where there is a steward of that ecosystem that acts of behalf of society i.e. a regulator.

[1] Resilience in Information Stewardship. I. Gheyas, D. Pym and J. Williams.

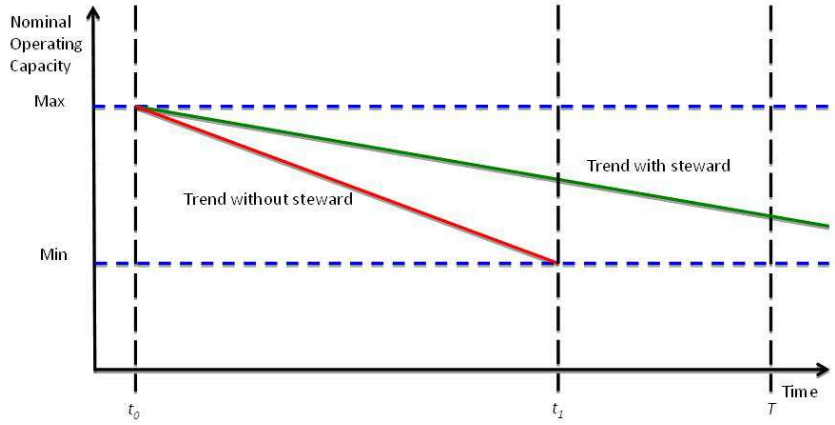


Figure 4 – Sustainability in an ecosystem with stewardship

In a general sense, it is expected that the 'Operating Capacity' of the organisation drops over time perhaps as the security controls become less effective against the increasing threat, steadily increasing level of technology and attacker capability/motivation, thus the CNI operator becomes less secure over time. The general view from other industries is that without a steward, the CNI operator will become less secure faster than when there is a steward in place (as shown above in Figure 4).

Next we introduce the idea of 'shocks' into the model. The purpose of an organisation investing in security controls is to guard and protect it from attacks and accidents. A shock can be an event or circumstance which drops the level of Operating Capacity of the organisation. As our models are focusing on security this is interpreted as a drop in the CNI operator's security posture. For examples such shocks could include:

- A change in technology e.g. a major cryptographic protocol is broken
- New vulnerability in the core CNI systems e.g. the Electricity Management System
- A change in behaviour of the target CNI operator e.g. a change in the regulatory structure that results in changes to the incentives of the organisation to the detriment of the ecosystem.

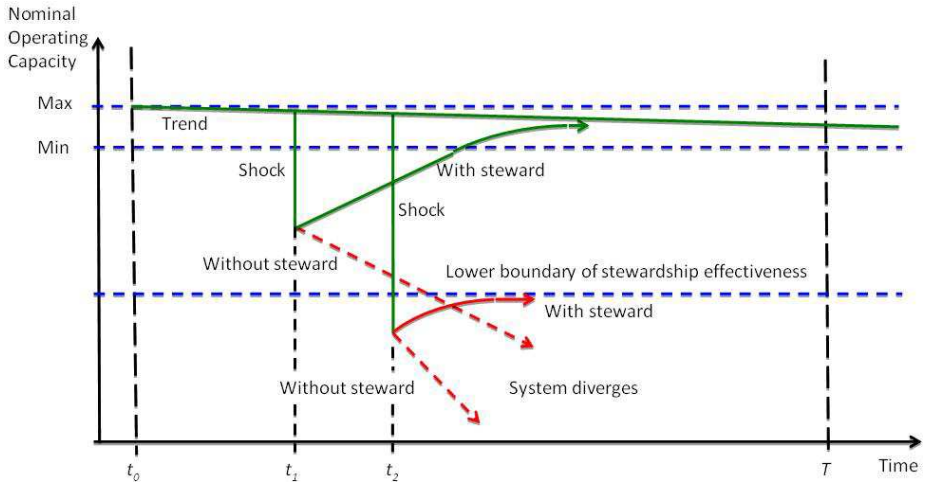


Figure 5 – Resilience in the ecosystem under different shocks

Figure 5 depicts four different types of shocks to the ecosystem which can be categorised as follows:

- Manageable shock without a steward that deviates from trend
- Manageable shock with a steward that helps return the CNI operator back to the prior level of operating capacity
- Unmanageable shock without a steward that deviates from trend sharply
- Unmanageable shock with a steward that thwarts the deviation from trend but cannot bring the CNI operator back to the prior level of operating capacity.

The purpose of the steward is to return the organisation back to the trend Normal Operating Capacity. The model aims to measure how resilient the CNI operator is at keeping within the bounds of the Normal Operating Capacity, whilst being subject to shocks and with stewards from different regulatory systems.

There are numerous articles on sustainability and resilience in information stewardship (e.g. Sustainability in information stewardship[2]) with detailed construction of models. To answer Question 1 the models need to have relevance in the case of a CNI operator and its regulator as the steward. To that end, the model needs to be calibrated with information from National Grid (as a CNI operator). This information fits into three areas:

- Discount rates: To understand the discount rate of National Grid it is essential to know how it decides which security risks should be mitigated first and which can be left until later. Following this, an understanding of the actual risk priority.
- Security Investment Plan: To understand National Grid's process of determining the priority of investing in certain security controls.
- Shocks: To get National Grid's view of how often 'unmanageable' shocks have occurred with the potential to directly or indirectly affect it, or the wider industry, at that time or in the future.

3.1.2 Agility systems model

Unlike the Sustainability and Resilience model, this model looks in more detail at the interactions of the CNI operator in response to the regulatory system and ongoing information or cyber security attacks.

The Agility model is built as a Stackelberg game (one of the simplest game-theoretic constructions). This game proceeds along the following steps:

1) The regulator (policy maker, P) chooses a regulatory system or policy regime by choosing whether it rewards attention to risk or compliance with rules (risk/rules weighting, w), a set of rules and an allocation of funds to the CNI operator (firm, F)
2) The CNI operator reacts by choosing its own allocation of funds (budget and set of security controls applied)

[2] Sustainability in information stewardship: Time preferences, externalities and social co-ordination. C. Ioannidis, D. J. Pym and J. M. Williams. In the 12th Workshop on the Economics of Information Security (WEIS 2013).

3) The choice by the CNI operator has an effect (subject to random fluctuations relating to the arrival of 'new' vulnerabilities) on transmission performance and compliance; both the regulator and CNI operator have preferences regarding such things, as represented by the loss functions of the regulator (L_P) and the CNI operator (L_F)
4) The regulator should anticipate the reaction of the CNI operator and set the regulatory structure accordingly.

There are a number of mathematical components of this model that, together, make up the Stackelberg game. These have been presented diagrammatically in Figure 6 below.

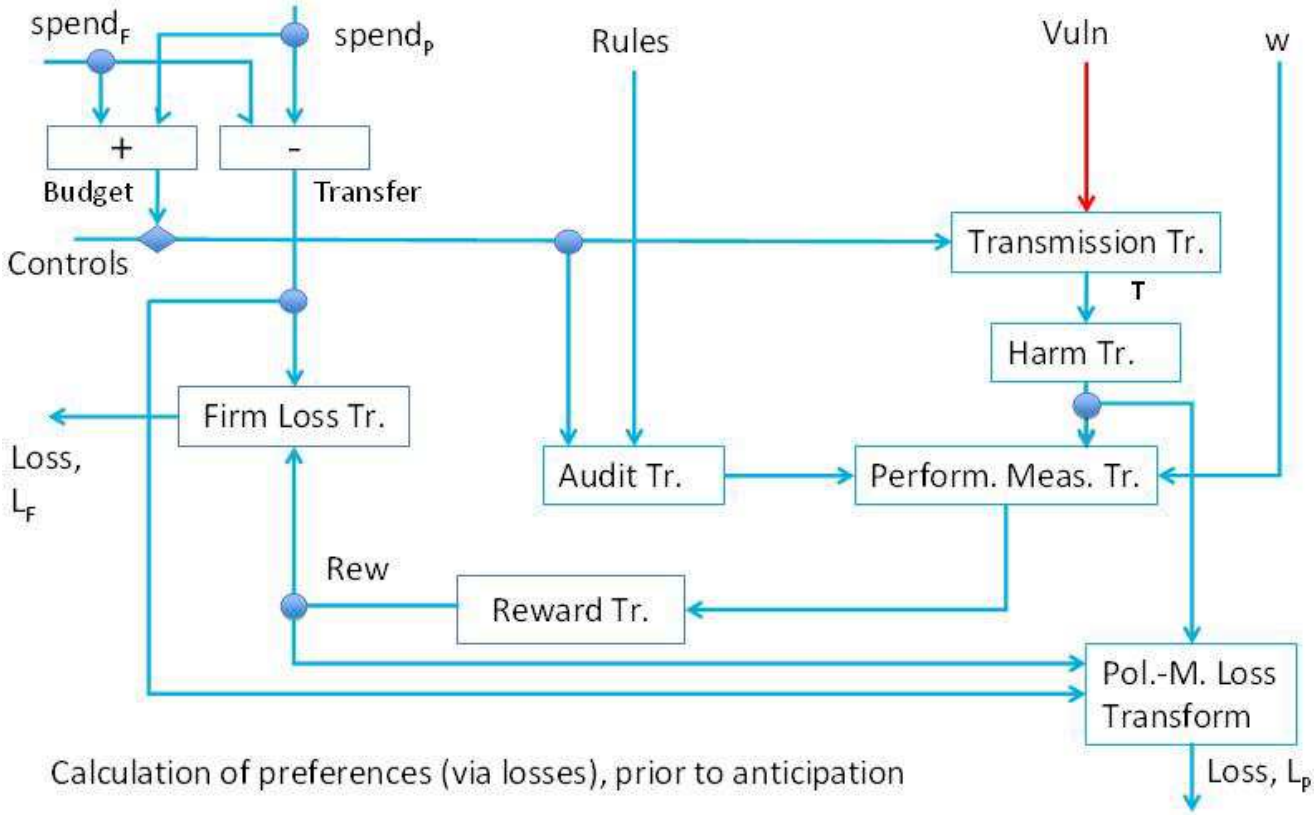


Figure 6 – Agility systems model as a block diagram

Each block (or transform) in Figure 6 represents a different set of mathematical functions which have a different objective. These are described in the table below.

Table 1 – Description of the components of the Agility Model

Input or Transform	Description
Rules	This is the set of rules from the regulator which could simply be high-level risk-based principles on one hand, or detailed rules on the other that the CNI operator must follow.
Vuln	This is the level of threats or vulnerabilities to Electricity Transmission. In the case of vulnerabilities, this could be a new vulnerability that is identified within Electricity Transmission that is yet to be exploited. For threats, this could be attackers attempting to exploit vulnerabilities whether successful or otherwise.

Controls	This is the set of security controls that the CNI operator implements on the Electricity Transmission system.
Transmission & Harm	Describes the state of the Electricity Transmission network and how it is operating i.e. whether it is coming to any harm such as operating outside of its tolerances.
Audit	Evaluates the level of compliance of the CNI operator to the rules set by the regulator.
Performance Measure	Takes input from the Audit and Transmission Harm transforms to measure the CNI operators level of performance.
Reward	Converts the output of the Performance Measure Transform into reward which is measured differently depending on which perspective the performance of transmission is being looked at.
Firm Loss	Describes the overall loss to the CNI operator taking into account of the output of the Rewards Transform and offsetting it by the transfer of the spending by the CNI operator and the Regulator.
Policy Maker Loss	Describes the overall loss to the Regulator as a proxy for society as a whole. It takes into account of the output of the Rewards Transform and offsetting it by the transfer of the spending by the CNI operator and the Regulator. In addition, it also takes into account of the actual harm to the Electricity Transmission network.

To make this model an accurate representation of a CNI operator each transform described above needs to be calibrated using information from National Grid. Rather than approach each transform in turn some high-level questions were developed that would help with the calibration and validation process in addition to calibration areas for the Sustainability and Resilience models:

- How much effort does National Grid put into complying with regulation versus actually mitigating risk?
- How do rewards or punishments (by the regulator) really affect what National Grid does in security?
- Without specific rules, what would the regulator really care about e.g. National Grid's security maturity etc?
- What does National Grid think their alternative measures of security are?

3.1.3 Sustainability, Resilience & Agility – One View

Above we have discussed the Sustainability & Resilience and Agility models from NGRID's perspective. In Figure 7 below, we show in an information graphic a depiction of how the two different models are being used to attempt to answer Question 1 from different stand points, and how the outcomes of these models will be brought together.

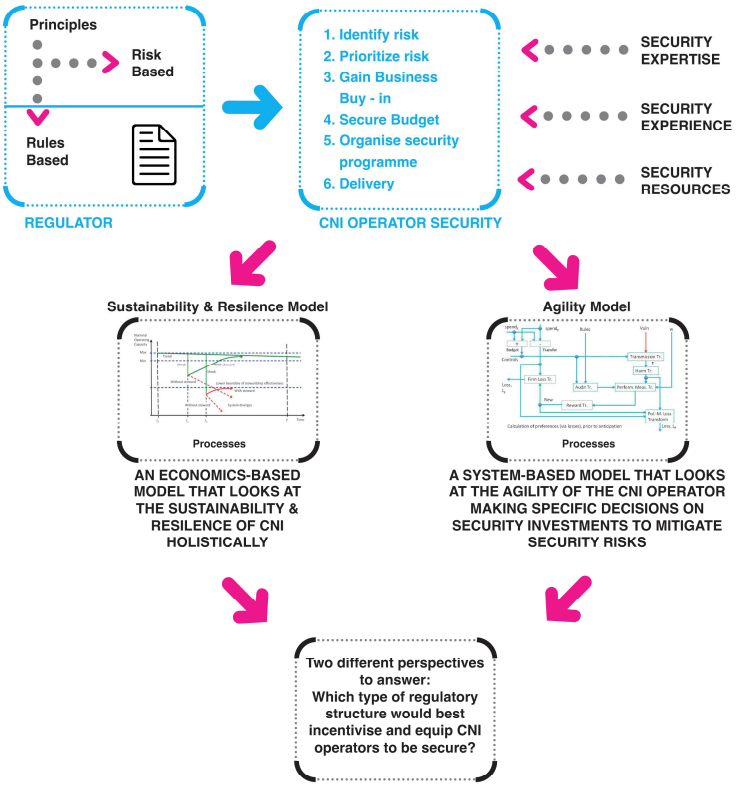


Figure 7 – Infographic: How the Sustainability & Resilience and Agility models are answering Question 1 and their outcomes will be brought together.

3.2 Question 2 – Society's views of security of CNI (WP4)

As we have discussed, 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. Nonetheless, CNI concern citizens indirectly but very profoundly. The role of CNI is often difficult to comprehend for citizens and society in general. Thus one of the biggest challenges for the study of citizens' perception of security measures in the CNI field was to identify issues which relate as close as possible to CNI, yet would be transnational and possible to study using the method of comparative media analysis.

Therefore, a meeting between NGRID and ISASCR took place in November 2012 to first determine whether there are or have been cases where information/cyber security issues in CNI have been noticed and discussed in wide scale media.

The most significant case in recent times has been the media reporting around Stuxnet, a piece of malware that was used to attack an Industrial Control System in Iran. More details around the Stuxnet (Malware - computer worm) attack can be found in

Deliverable D2.3. Due to the potential impact of a successful attack using malware like Stuxnet on an industrial control system, as used in many CNI industries, the media took notice of this particular malware and reported on it significantly. The media brought it to the attention of society in general and thus the views of society around the security of CNI became evident.

Using the methodologies and techniques of WP4 we wanted to perform a comparative analysis on the different views (societal and expert) of the Stuxnet malware utilising different media sources from different countries. This comparative analysis is based on the idea of 'salience'. Salience is defined as the public perception and reception of security issues and, more specifically, of security measures; for this purpose salience signifies the degree of acceptance (positive salience) and the degree of rejection (negative salience). Media salience has been used in the comparative analysis, either positive or negative, as an indicator of the potential acceptance of security measures.

In Figure 8 below, we show in an information graphic a depiction of the different facets of the Stuxnet malware and its effects on policy makers.

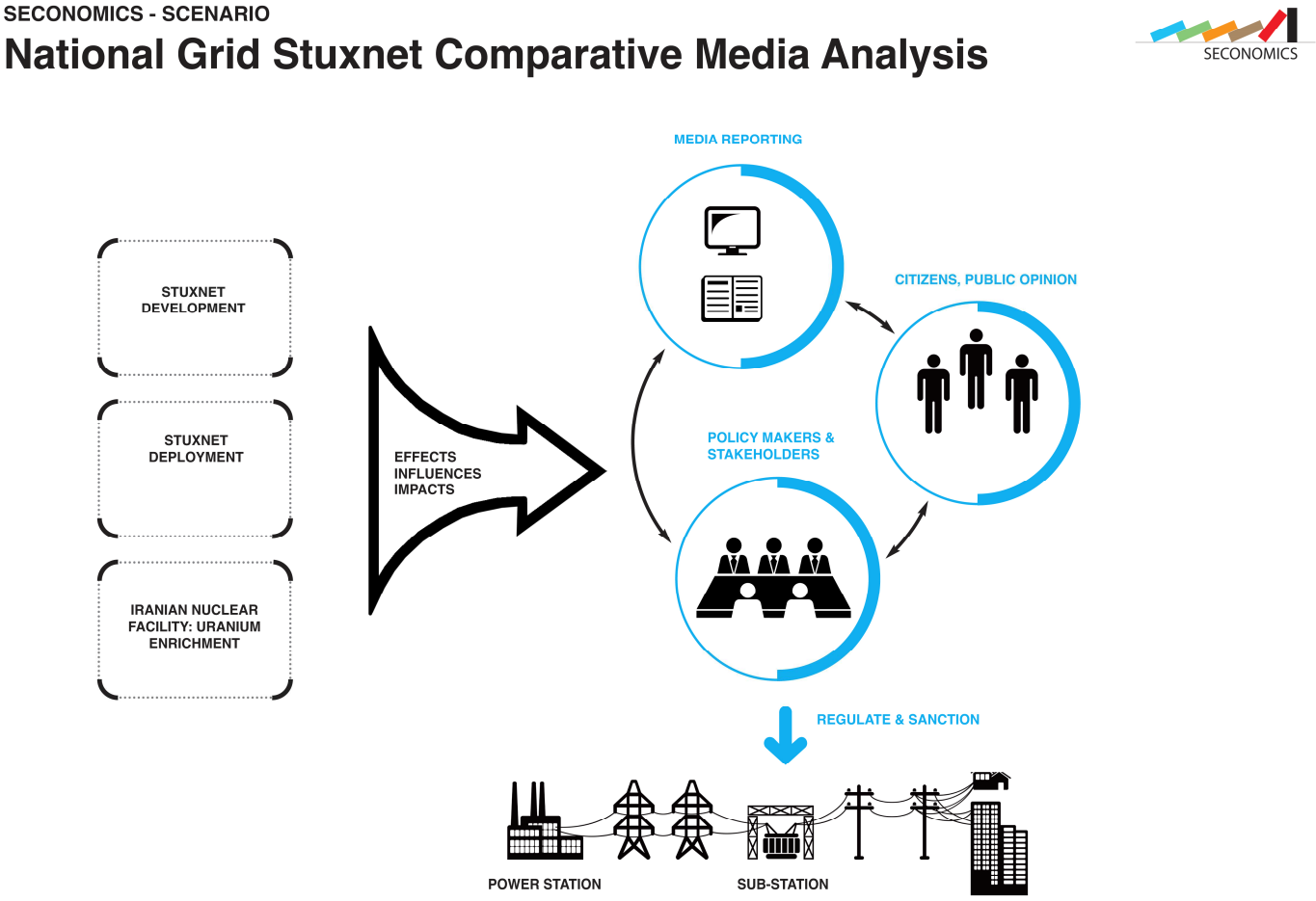


Figure 8 – Infographic: The facets of the Stuxnet malware and how it has effected societal views.

More details of the specific comparative analysis methodology can be found in Deliverables D4.2 and D4.3 and a summary of the results of the analysis for the Stuxnet malware are presented in the next section.

3.3 Model Building Processes and Activities

The economic and systems models 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 includes the analysis, calibration, validation and refinement of the models, see Figure 9 below.

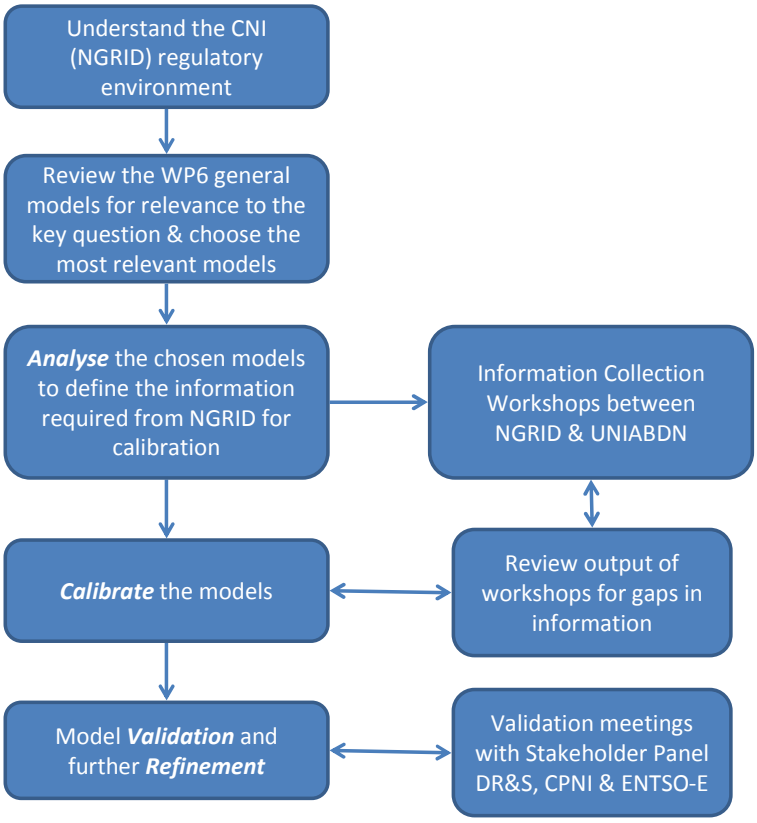


Figure 9 – Model Building Workflow.

The workflow above shows the different stages of model building and the interaction between the project partners and members of the stakeholder panels. A number of information workshops between different parties were held to gather information and data to be fed into the analysis and calibration of the models prior to the validation steps. These are detailed in the table below.

Table 2 – Information Workshops and meetings

Date	Workshop / Meetings
7th November 2012 Madrid, Spain	Meeting between National Grid CISO and Research Manager and ISASCR to identify and review significant cases where information/cyber security issues in CNI

	have been noticed and discussed in wide scale media.
9th January 2013 Boston, US	Workshop on National Grid's experience of NERC-CIP Compliance in the US with Compliance Managers in National Grid, Massechussets, US. Detailed notes were recorded and a redacted version can be found in Appendix 1.
23rd April 2013 London	Workshop between UNIABDN and members of the DR&S leadership including the National Grid CISO. Detailed plan of questions for the DR&S leadership were agreed between the NGRID Security Research Manager and UNIABDN. These can be found in Appendix 2.
19th - 21st May 2013 Aberdeen	Workshop between the lead NGRID Security Research Manager and UNIABDN. Focus was to share and discuss NGRID confidential information for the purposes of model calibration.
3rd - 5th September 2013 Aberdeen	Workshop between the lead NGRID Security Research Manager and UNIABDN. This workshop was to go other the initial construction of the models with the focus to check the previous calibration against the real-world CNI case study.

4. Model Validation

The next stage in the modelling work is to validate and refine the models. This section presents the validation criteria (defined earlier in the project), activities and results. Finally, additional dissemination activities are presented.

4.1 Validation criteria

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 as a matrix between the validation objectives (columns) and the Seconomics outcomes (rows) that were relevant to the case study. In the table below we present the validation criteria for the CNI case study but focus on the Seconomics Outcomes that are relevant to Years 1 & 2 of the project.

Table 3 – CNI Case Study Validation Criteria (Extract)

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

4.2 Validation Activities

Whilst there are references to the case study's national and supranational stakeholders, that validation will be achieved in the final year of the project as we disseminate the refined models to those stakeholders. This is discussed further in Section 6. Instead our focus here is on the subject matter experts in security within National Grid, namely the Digital Risk & Security (DR&S) Leadership.

DR&S are tasked with managing and mitigating the cyber security risks within National Grid globally (UK and US) through security strategy, governance, risk, compliance, consulting, architecture, threat and incident management. DR&S is headed by National Grid's Chief Information Security Officer (CISO) who is also the main sponsor of the

company's involvement in the SECONOMICS project. Directly reporting into the CISO are DR&S heads of department who lead the different areas of security. The CISO and his direct reports for the DR&S leadership whose mission is to secure National Grid today and in the future.

Part of securing National Grid includes understanding and shaping what the security regulation of the future will look like. Hence, DR&S are a key stakeholder in the work of WP2, as described in deliverables D2.2 and D2.3. In the table below we present the validation meetings that took place.

Table 4 – Information Workshops, Validation and Calibration meetings

Date	Workshop / Meetings
26th November 2013	National Grid Validation Meeting 1 with the DR&S Leadership. Focusing on the Agility model, Stuxnet media analysis and partially on the Sustainability & Resilience model. Details of the meeting and attendees are provided in Appendix 3.
27th January 2014	National Grid Validation Meeting 2 with the DR&S Leadership. Focusing on the Sustainability & Resilience model and partially on the Agility model. Details of the meeting and attendees are provided in Appendix 4.

4.3 Validation Results

With the validation meetings in mind, in the table below we present how the model validation activities and outcomes have met the validation criteria presented in the Table 3 above.

Table 5 – CNI Case Study Validation

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 help focus all workshops.	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 positively be the ENTSO-E CIP group in November 2012 and then the CSP group in April 2013.	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 the UK and was thoroughly detailed in deliverable D2.3.
Security risk, socio-economic and system models	All models are built upon well-defined general models accepted by the academic community. An initial view of the models were presented to the CPNI at the SCSIE meeting in	The Sustainability & Resilience and Agility models are built upon the detailed information in deliverable D2.3 and evidence drawn from a number of workshops and	The results of the models are still in the initial phases. A variety of potential results and outcomes of the models were run past the DR&S leadership in the Validation

	January 2013 and were received with positive feedback. Detailed models were presented and accepted by the DR&S leadership at the Validation meetings. Further validation with the supranational stakeholders is planning for in M29.	meetings between the UNIABDN, UDUR and NGIRD. The models inherently integrate the security, economic and social perspectives. Further agreement of the models with the CPNI and ENTSO-E are planned for M28 and M29.	meetings and it was agreed they were relevant and could be turned into policy and regulatory recommendations to meet the aims of WP2 and Seconomics.

Next we go into more detail around the validation outcomes of each modelling stream namely WP6 and WP4.

4.3.1 WP6: Economic & System Models

For the Sustainability, Resilience and Agility models significant input was required from DR&S, in the first instance, in order to calibrate the models and gain buy-in. The purpose of gaining buy-in at this stage is to maximise the potential value to the National Grid CNI stakeholders of the outcomes and recommendations that come from the models.

Overall the DR&S leadership were happy with the approaches being taken in the Sustainability & Resilience model and the Agility model. After a discussion of the potential outcome of the models they were broadly happy that these models could help to assess the effectiveness of the different regulatory structures and, in turn, help to provide recommendations on what type of regulatory regimes would work best to incentivise CNI operators to be secure.

In particular they were very interested with how the input to the models around the type of regulation (Rules-based, Risk-based or hybrid) could be changed on-the-fly. The purpose of this would be to see what the outcome would be to the security and operation of the Electricity Transmission network overall and the specific loss to the organisation and the regulator.

The next step was to discuss the areas of calibration of the models. The following information obtained for the purposes of calibration is organised as per the key areas in Sections 3.1.1 and 3.1.2.

- Discount rates: the DR&S leadership provided corporate insight as to how security risks are prioritised for mitigation given the limited resources. They mentioned that it is essential that the business buy-in to the risk before it can be resolved, regardless of its severity.
- Security Investment Plan: the DR&S leadership discussed their internal process of prioritising and delivering security controls within the business. Specifically they focused on the careful balance of quick-wins, fast tactical response versus slow but more effective strategic response and security resources in order to have a successful security delivery programme.
- Shocks: a clearer definition of shocks was agreed to be those unexpected events with potentially large impact to the CNI operator and beyond. A number of events

that could be considered shocks from the recent past were discussed and this will help the academic partners gauge the frequency and size of such events.

4.3.2 WP4: Comparative Media Analysis of Society's views of Security of CNI

ISASCR comparative media analysis was focused on the perceptions of citizens and society. As a result, the topics of analysis in the Airports and Urban Public Transport case studies were the 3D Body Scanner and CCTV respectively. Whilst different, the Stuxnet case has a special position amongst the other two topics due to its technical character, which led to dominance of the debate by state officials and experts (with journalists providing statements of mostly explanatory character) and the public and various civil society groups marginalised. In terms of intensity as well as the nature of media reporting, the United States was indisputably the leading country setting up the agenda for others. Media in other countries being studied followed the US debate, firstly by informing the readership about the character of the malware and explaining the situation and secondly, by evaluating and analysing events that had occurred.

Three interconnected perspectives were typical for media coverage of Stuxnet in counties under study (for more insights see table 6 below and for details see D4.3). First, and prevailing, perspective was purely informative where newspapers described the Stuxnet malware, its functions and deployment as well as described the Iranian nuclear program. In the second perspective, the Stuxnet incident was framed to the global cyber security context, industrial espionage and cyber war. On this "macro" level, newspapers informed their readers about the wider consequences and negative impacts of the Stuxnet attack on geopolitical stability such as potential counterattack and they discussed the legitimacy of cyber-attacks in regard to international law. The third perspective, present in a few countries only offered a marginally new and more sophisticated viewpoint on Stuxnet, contextualizing it in the context of the other methods of surveillance and tracking of personal data.

Table 6 - Categorisation of Stuxnet related topics according to salience 2010-2013

	Attack on Iran	Iranian uranium enrichment program	Deployment/ attack using Stuxnet	Stuxnet	Cyber war
High Salience	Spain	UK	USA	USA	Spain
	Great Britain	USA	Slovakia	UK	Czech Republic
		Slovakia	Spain	Germany	USA
		Spain			UK
Medium Salience	Slovakia	Poland	Italy	Czech Republic	Germany
	Germany	Czech Republic	Mexico	Italy	Poland
	USA			Mexico	Italy
					Mexico
Low Salience	Czech Republic	Germany	Germany	Spain	
	Italy	Italy	UK	Poland	
	Mexico	Mexico	Czech		

			Republic		
	Poland				

To summarize the results of our media salience analysis, in some countries such as the United States, Germany and partially also in Slovakia all these three perspectives or levels of media perception on Stuxnet were present. Generally speaking these were sophisticated and detailed debates. However, in most of countries - especially in the Czech Republic, Poland, UK, and in Spain media coverage of Stuxnet was reduced to one or two of the above described perspectives. Media in these countries provided mainly descriptive articles on Stuxnet issue but wider context and justifications of presented arguments were missing. In other words, across all countries, any form of broader debate about the potential consequences and impacts of cyber-warfare on CNI were mostly missing.

As a supplement to the printed media analysis, we chose four English-language expert security blogs to gain deeper insight into the communication patterns of those inside the security expert community. Increasingly important, blogs are more and more portrayed as community forums or political outlets, as opposed to the initial understanding of blogs, as forms of personal self-expression. There is also strong evidence that media elites – editors, publishers and columnists – consume political and expert blogs (Drezner and Farrell 2004[3], 2008[4]), indicating a connection between the political and expert blogosphere with mediasphere. This makes reputable blogs even more relevant and influential within the general media context (for the full report see Annex 8 of D4.4). The four English-language security expert blogs selected for this analysis were Bemosa, Roger-Wilco, Hack in the Box (HITB) and The Register.

In the expert blogs, Stuxnet was the most salient topic. It accounted for almost 70% of the overall relevant articles. The topics discussed by experts were mostly cyber war (14.2%), Stuxnet itself (13.6%), followed by themes such as attack on Iran, USA, Israel, the development of Stuxnet and its deployment. The vast majority of articles were expert insights into these issues. This is also visible in general lack of justification (experts did not see the need to justify informative statements), with the exception of efficiency, defense and preemptive strike as reasons for the development and deployment of Stuxnet.

This comparative analysis confirms, that unlike the other two security issues under study, CCTV camera systems and 3D body scanners, CNI as exemplified by Stuxnet is not a technology infrastructure that the common person is aware of or has an opinion on regarding its security and is thus not in the focus of the media. The framing of Stuxnet is shaped by the fact that its aim is not to improve security of individuals by monitoring public places as CCTV camera systems or detect weapons and prevent from terrorist attack as 3D body scanners. Specifically, the Stuxnet malware is a weapon in itself, developed not to protect CNI but to destroy it. From all of the three security topics

[3] The Power and Politics of Blogs. Daniel W. Drezner and Henry Farell. Paper presented at the American Political Science Association 2004, Chicago, IL, September 2004.
[4] The Power and Politics of Blogs. Daniel W. Drezner and Henry Farell. In Public Choice 134 (2008): 15-30.

involved in our comparison, Stuxnet has the greatest impact on geopolitical stability and questions of international law and security. Therefore, this topic is highly relevant not only for global security context on a macro level but also for security of individuals although this saliency on micro level seems to be indirect and even marginal and the actors engaged in the debate are mostly experts and politicians.

The summary results of the comparative media analysis of the Stuxnet malware were presented to the DR&S leadership in the validation meetings. Due to the limited awareness of CNI by citizen's and media alike, the DR&S leadership were keen to understand what views the media took of the Stuxnet attack given the internal ramifications within National Grid following the Stuxnet incident in 2010. The group were not surprised by content of the media reporting of Stuxnet particularly in the expert blogs but were surprised by some of the countries where there was a significant salience. More details of the analysis are planned to be presented to the key stakeholders in future validation and dissemination events.

4.4 Additional Dissemination Activities

In addition to the information workshops (Table 2), validation meetings (Table 4) and other meetings with members of the CNI Stakeholder Panel (Table 8), a number of dissemination activities have taken place between M1 and M24 with other interested parties. These are summarised in the table below.

Table 7 – Additional Dissemination Activities

Date	Audience & Venue	Workshop / Meetings
26th April 2013	CESG Cheltenham, UK	Presentation on SECONOMICS to the UK Intelligence Services focussing on the work completed on the CNI case study during Year 1 of the project.
1st - 3rd May 2013	6th International Electricity Infrastructure Assurance (IEIA) Forum Vancouver, Canada	Presentation on the CNI security threats work completed during Year 1 of the project to industry and governmental organisations involved in the operation and security of electricity infrastructures.
16th - 18th September 2013	8th International Conference on Critical Information Infrastructures Security (CRITIS) 2013 Amsterdam, Netherlands	Discussion on the SECONOMICS project and the aims and future work of the CNI case study during panel discussions.
10th - 12th March 2014	81st International Information Integrity Institute (I-4) Forum Phoenix, USA	Presentation on SECONOMICS and the work completed to date in the CNI case study to the Security Leaders of major organisations across the world. This includes financial institutions, utilities, oil & gas and manufacturers amongst others.

5. Future & Emerging 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 D2.3, the future and emerging threats and risks to CNI were broken down into different views which looked at the impact, opportunity, threat actors & motives and means. National Grid's overall opinion was that the future landscape of energy delivery was changing with the development and implementation of smart grids and SCADA systems becoming more complex and interconnected. As a result the threat landscape would increase in future. To add to this, with the continued fast paced implementation of IT within remote control equipment, the opportunities attackers will have in the future to compromise CNI is continually increasing. Finally, an increasing sophistication of threat actors with higher capabilities and motivation to attack CNI can be expected in the future.

This expert view of the future and emerging threats plays directly into the building and calibrating of the models discussed in the earlier sections. In particular:

- For the Sustainability & Resilience models, the future and emerging threats feeds directly into the understanding of shocks. By looking at recent shocks in security (with potential impact on CNI) the DR&S leadership provided their expert opinion on how frequent and how severe future and emerging threats would be. This expert opinion has helped to driving the calibration of shocks within this model.
- For the Agility model, future and emerging threats has a direct bearing on the 'Vulnerability' input into the model. Through expert opinion the academic partners are able to gauge the frequency, severity and, importantly in this case, the type of future and emerging threats that could occur, thus affecting the outcome of the model.
- For Society's view of security in CNI, a detailed understanding of the Stuxnet malware has aided in the appreciation of the outcome of the comparative analysis. This particular threat was given such high weight as the DR&S leadership's expert opinion is that in the future use of malware to attack industrial control systems will only increase. Therefore, understanding society's view of the Stuxnet incident would aid in the government's and regulator's media handling of such future events.

6. Pan-European Coordination

In D2.3 we presented the different stakeholders in the CNI case study and a plan to engage with those stakeholders. The stakeholders were organised into the following groups: internal National Grid, national and supranational stakeholders. Earlier we discussed in detailed how we have engaged internally with the National Grid stakeholders (DR&S) gaining validity of the models and making significant progress towards calibrating them. The next step is to engage wider, in line with the plan set out in D2.3.

The two main external stakeholders are the Centre for the Protection of National Infrastructure (CPNI) in the UK, as the national stakeholder, and the European Network of Transmission System Operators for Electricity (ENTSO-E) Cyber Security Protection (CSP) and Critical Infrastructure Protection (CIP) subgroups. For maximum buy-in of these stakeholders, into the aim of the research within this case study and the subsequent modelling work, it is essential that the stakeholder groups are taken on a journey of awareness of SECONOMICS during the life of the project. By engaging with the stakeholders in this way, we maximise their understanding before the modelling work is thrust upon them and their input into assessing the validity of the models and ideas for bringing this research to the attention of the regulators at a national and supranational level. To this end, a number of presentations on the CNI case study have been given to these stakeholders to date and these are detailed in the table below.

Table 8 – Past engagement with key national and supranational stakeholders

Date	Meeting	Description
14th November 2012	ENTSO-E CIP Group meeting	This group brings together the senior security professionals from the various Electricity Transmission System Operators across Europe. As this meeting was early in the project, a high level presentation was given about SECONOMICS and the planned worked in the CNI case study.
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.
3rd April 2013	ENTSO-E CSP 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.
7th November 2013	ENTSO-E CSP Group meeting	A short presentation was given to the group reminding them about the SECONOMICS project and an update on the modelling work.

The next steps are as follows:

1) To engage with CPNI directly to further motivate the key aims of the CNI case study, present the progress of the modelling work and some initial outcomes. The key part of the engagement is to disseminate how this could influence future regulation implemented by the Department of Energy and Climate Change (DECC), the regulator for National Grid.
2) To continue the engagement with the ENTSO-E CIP and CSP subgroups to present the progress of the modelling work and some initial outcomes. The focus here is to show how this work could help influence each Transmission Service Operators national regulator and the European regulators.

7. Conclusion

This report builds on the work in Deliverable D2.3, National Grid Requirements, the modelling framework in WP6 and the media comparative analysis methodology in WP4. Through recapping the regulatory structures that National Grid adheres to in the UK and US, the key questions and aim of the CNI case study were presented and further motivated, which are:

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

The report then describes the different modelling techniques that are being utilised, principally from WP6, to assess the effectiveness of the different regulatory structures at incentivising CNI operators to be secure. In addition, the method and process of the comparative media analysis by WP4 was summarised.

In particular we are using an economics and systems modelling approach and are making these general models specific to the CNI setting through validation and calibration with the DR&S leadership. A high-level summary of the model validation and calibration activities were presented with a focus on the outcomes of the validation meetings with National Grid's DR&S leadership. Also, the outcomes of the comparative media analysis on the societies view of security within CNI were presented along with the headline results.

Following this, the pan-European activities were described. Specifically the next steps were presented which centres on the calibration and validation activities with the key stakeholders outside of National Grid, namely CPNI and the ENTSO-E Critical Information Protection group.

8. References

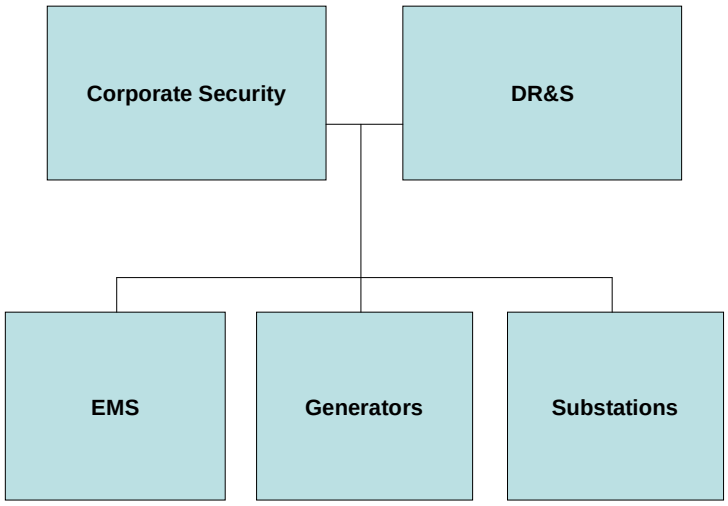
1. HMG Information Assurance Standard No. 1 – Technical Risk Assessment v3.51. CESG – The National Technical Authority for Information Assurance and the Cabinet Office (2009).
2. Resilience in Information Stewardship. I. Gheyas, D. J. Pym and J. M. Williams.
3. The economics of information security investment, Lawrence A. Gordon Martin P. Loeb ACM Transactions on Information and System Security (TISSEC) TISSEC Homepage archive Volume 5 Issue 4, November 2002, Pages 438 - 457, ACM New York, NY, USA
4. Sustainability in information stewardship: Time preferences, externalities and social co-ordination. C. Ioannidis, D. J. Pym and J. M. Williams. In the 12th Workshop on the Economics of Information Security (WEIS 2013).
5. The Power and Politics of Blogs. Daniel W. Drezner and Henry Farell. Paper presented at the American Political Science Association 2004, Chicago, IL, September 2004.
6. The Power and Politics of Blogs. Daniel W. Drezner and Henry Farell. In Public Choice 134 (2008): 15–30.

Appendix 1 – National Grid NERC-CIP Workshop Detailed Notes

Below are the redacted notes from this workshop.

Introduction

US Transmission is regulated by NERC-CIP



3-Yearly audits are conducted on a corporation rather than specific infrastructure.

NG has 8 corporations, which are audited separately:

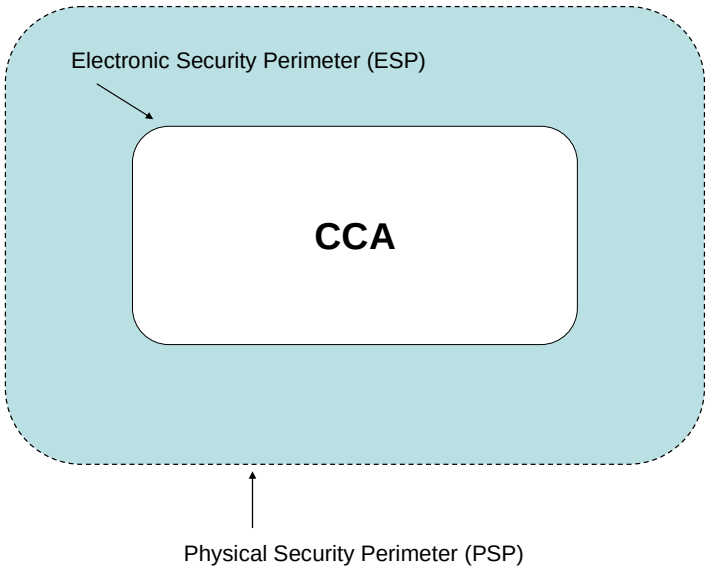
1) Massachusetts Electric Company
2) New England Electric Transmission Corporation
3) New England Hydro Transmission Corporation
4) New England Hydro Transmission Electric Company
5) New England Power Company
6) Niagara-Mohawk Power Corporation
7) Narragansett Electric Company
8) NG Generation LLC

For each audit the relevant corporation needs to complete Reliability Standard Audit Worksheets (RSAWs). One RSAW is completed per CIP standard.

The CIP-002 standard describes the process of compliance:

- Critical Assets (CAs), e.g. substations, generators, control centres, needs to be identified first.
- Then Critical Cyber Assets (CCAs) (e.g. racks, servers, mainframes) which are 'essential' to the operation and security of the CA have to be identified for each CA.

For each CCA two perimeters must be defined as shown below:



Prior to an employee/contractor getting access to the CCA, the requirements are as follows:

- A Personnel Risk Assessment (PRA) background check (vetting)
- Relevant Training
- Person requires a Business Need to access the CCA.

Whilst violations do not all lead to fines and most fines are quite small, this is not National Grid's (NG) motivation to avoid violations. The reason for avoiding violations is rather to maintain NG's reputation with its regulators and customers. If the event should occur, that NG gets many violations, this would cast a damning light on the company and the management.

Since 2010 NG has been through a number of audits. The NPCC audit team consists of:

- Firewall and Technical IT experts
- Physical security experts
- Process and procedure experts.

Often the same auditors have come back on subsequent audits.

Questions and Answers

1) Which are the most important parts of the NERC-CIP regulatory framework?

- The physical protection forms an important part of CIP. There are no requirements for cameras at PSPs, but it seems like this should be required, i.e. for the entry doors at control centres.

- Another important issue is the cyber access. This includes who can get access physically and electronically.
- Alerting is also an issue as the standards do not require an alert if someone gets access to a CA.

2) What are the regulator's and NG's view of compliance?

- Compliance Application Notices (CANs) are documents that interpret the standard for the auditors
- There is a difference in views of the standard between NPCC and industry.
- ***SOME NOTES REMOVED***

3) How does the regulatory regime affect the way in which NG operates? What does NG not do in terms of security because of NERC-CIP?

- The rules for access to CCAs seem good and certain areas of the business wanted to apply that to the information held in CCAs as well. ***SOME NOTES REMOVED***
- Operational technology folks, specifically in substations, are often of an engineering background rather than an IS background. As a result their work practices are different. More work and effort is required to bring them to the level of NERC-CIP, e.g. when IT boxes are replaced an engineer would simply replace the box with a new one and bin the old one. No testing would be carried out or documentation completed as to the changed kit.
- Secure Remote Access was removed from CNI IT systems because the rules of NERC-CIP were too difficult to obtain.
- Prior to NERC-CIP there was a 'free-for-all', no change control and limited (out of date) documentation. However, after NERC-CIP became mandatory there has been a cultural change in terms of security, documentation has to be complete and up to date, accountability has to be clear and documented as well as self-auditing has to be in place.
- Information protection internal audits are required yearly and access to CCA audits is required quarterly. However, it was thought more business efficient and cost effective if both are done quarterly.
- Some CNI operators are using older techniques to get around having to be NERC-CIP compliant, e.g. RTUs have serial or IP connectivity, whilst it is better to have IP connectivity, serial connectors have been used as these do not have to be CIP compliant.
- By passing an audit, the NG leadership often thinks NG is fine in terms of cyber security. This can slow down or even stop the implementation of important new or upgraded security controls as further actions are not taken in consideration and the current state is thought as being sufficient. Internal audits, by external parties are used to help send the right message to NG leadership.
- To protect NG, a dedicated lawyer who is a NERC-CIP expert, needs to be present during audits (this is an additional cost).
- The changes between the versions of CIP can cause issues when controls need to be implemented, e.g. money does not want to be spent securing a CCA to CIPv4, when the risk-based rating of the CCA in CIPv5 means the extra security would not have been required.

4) What are the operators' attitudes to NERC-CIP?

- Between audits, as the operations people are aware that auditors will be back, effort is put into completing important documents and getting them approved and signed. This positive cultural change has spread into other areas.
- Before NERC-CIP there was not a culture of security. Updating/producing documentation was a difficult and slow process, but now it is a day-to-day part of work although there are still some frustrations.
- Due to compliance concerns and possible fines, peer utilities companies are reluctant to share information for fear of the NPCC finding out. The NPCC does run a half-yearly workshop with all the utility companies to overcome this and NERC and FERC are also in attendance.

Issues

- Volunteers from utility companies help to write the NERC-CIP standards.
- Currently, either one is fully compliant or not compliant at all. But now if something is found and fixed using the rules of FFT this may not result in a violation.
- Currently, there is a more rules-based approach but the CIP standards are moving to a more risk-based approach in CIPv5, i.e. CAs are rated H, M and L.
- Protected asset vs. CCA: The rules are nearly the same so for a positive cultural change NG decided to tend towards assigning a cyber asset as a CCA.
- A lot of time is spent discussing with the auditors first, followed by discussions between the NPCC enforcement group and corporate. Also NG lawyers get involved in the process as well, particularly during audits. This process does not only cost a lot of time, but also has a financial impact.
- It takes lots of work to get a TFE approved, but once approved you have a 'get-out-of-jail-free card'. The NPCC may help write an organisation's TFEs as well. The original philosophy was that NERC-CIP would not require anything extra to be spent in order to be compliant, but this is changing with v5.
- National Grid has fragmented teams of CNI networks geographically, which means that each of them does compliance differently. A disadvantage of this can be to cause the auditors frustration.
- There is no guidance on how testing should be done, i.e. RTUs tested in development environments. The NPCC has the right to do readiness audits for the implementation of new systems e.g. EMS.

Positives

- Having a specific cyber security team helps with making senior management aware of risks, issues and important investments that are required in security.
- In emergency mode paperwork and documentation is in 'catch-up' mode. NERC-CIP and NPCC recognised this and therefore, NERC-CIPv5 takes emergency mode into account. This includes the potential to bring in vendors who are not CIP trained but are needed promptly and have the specific skills for the job.
- Other departments, such as gas, have improved their security posture as well, due to the implementation of NERC-CIP controls.

Acronyms

CA	Critical Asset
CCA	Critical Cyber Asset
CIP	Critical Infrastructure Protection
ESP	Electronic Security Perimeter
FERC	Federal Energy Regulatory Commission
FFT	Find, fix, track
NERC	North American Electric Reliability Corporation
NPCC	Northeast Power Coordinating Council
PRA	Personnel Risk Assessment
PSP	Physical Security Perimeter
RSAW	Reliability Standard Audit Worksheet
TFE	Technical Feasibility Extension

Appendix 2 – National Grid Workshop Questionnaire

For each question, where relevant

- What are the frequencies of information/cyber attacks?
  - Breakdown by size/style
  - Matrix style by magnitude (frequency in the data)
  - Notion of (and proxies measurements for) magnitude will vary greatly, depending on nature of vulnerable system and attack, important to include these for context.
- What is the mechanism of investment?
  - How is your budget spent? (breakdown of budget, buildings, people, equipment, projects).
  - How much does it change? (2 year period, 5 year period, 10 year period).
  - Can we get a picture of the growth curve for security investment, and as a percentage of operating costs?
  - When has the budget increased suddenly? Was it in response to an event or assessment of risk?
    - Has the business changed how much it spent on security as a function of what DR&S have told them? Or from external feed for instance CESG/DECC/CPNI?
      - Example patching client or network software or SCADA?
      - Vetting procedures changing?
  - What is the split of your total security effort between:
    - day-to-day operational security
    - strategic or other significant change
- Are year-on-year frequencies of events (attacks/risks) useful?
  - Defensive posture (the configuration of the security procedures the `tightness' of procedures).
- What about five-year period? (trend?)
  - What is your barometer for measuring how secure you are?
  - Is there any objective measurement, or is it purely an internal sense that the right people, (operational and meta-) processes and tech. are in place.

  - How do you measure where you are now versus where you want to be?
  - What is your capability maturity model?
  - What does your target level of security look like?
  - How often do you deviate from you target?
  - How many times do you sample and review risks?
  - How long is your policy time horizon (over what kind of timescales do you plan)?
  - If possible, what is the duration of return on assets needed for investment decision-making (commonly referred to as the payback period)?
  - Have you ever observed clustering of security incidents?
- Discount rates
  - How long does it take for you to amortize a security investment?
    - Payback period?
    - How frequently do you/plan to roll over security investment?
  - How long does it take the business unit to depreciate an asset?
  - How often do you replace kit?
- SCADA and control room
  - What are the risks?
  - How do the risks change?
  - How often do you change investment in security/security measures with respect to the SCADA and control room?
  - Do you have issues with the lack of diverse SCADA providers?
  - Does this lead to systemic risk?
  - Using the same technology or stuck with one contractor?
  - How does network communication innovations effect operational security?
  - How reliable/redundant is your network?
    - Communications network? Are there any situations in which you only have ONE communication linkage?
    - Concern `man-in-the-middle' attacks?
    - How secure are these networks?

  - Is there anything I'm missing?

- How do we gather knowledge/intelligence?
  - Is there any investment in intelligence gathering on threats?
  - How much is spent on consultancy to evaluate security risk?
  - How much is spent on monitoring operations? (I would like to include the business unit).
- Outsourcing and principal agent problems.
  - Which day-to-day services do you externally contract?
    - How many of these are critical services?
    - How many of these are security services?
  - How many externally contracted projects are run simultaneously?
  - How many of these are security projects?
  - Have you contracted out a project in response to generic security threats? How large compared to net revenue?
    - Understand NGs external contractors/consultants for CNI?
  - How often do you re-contract external projects or services?
    - Have you changed contracts in response to a security shock?
  - What are the types of penalty clauses for security failures are built into the contracts, if any?
- Policy imposition
  - How often do you change you global policies in response to policy re-statements in the US?
  - How are policy changes disseminated down to key stakeholders in the company?
  - What is the speed of adjustment in the business to new or re-stated regulations in the US?
  - How do policy rules constrain your behaviour?
  - How are you constrained to adapt to new risks?
    - Given the resources expended on compliance with existing rules?
    - How often are you constrained (frequency)?
    - How long does it take the regulator to adjust rules?

        - Are these adjustments sometimes pre-emptive?
    - In the UK how often do you adjust your security policy requirements?
    - How are your global policies affected by changes in the US regime?
- Of the effort/investment you spend on change, what is the split between:
    - Change to comply with rules and regulations.
    - Change driven by an internal assessment of risk.

Appendix 3 – National Grid Validation Meeting 1

Date: 26th November 2013

Venue: Club Quarters, 8 Northumberland Avenue, London, UK WC2N 5BY and via teleconference with National Grid Warwick, Warwick Technology Park, Gallows Hill, Warwick, Warwickshire, CV34 6DA.

The following people were in attendance at the Initial 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
Steve Collins	NGRID	Chief Information Security Officer
David King	NGRID	Head of Security Strategy, Policy & Architecture
Lawrence Russell	NGRID	Head of Business Security
David Pym	UNIABDN (University College London)	Head of Cyber Security Research at National Grid

Appendix 4 - National Grid Validation Meeting 2

Date: 27th January 2013 at 14:00

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
Steve Collins	NGRID	Chief Information Security Officer
David King	NGRID	Head of Security Strategy, Policy & Architecture
Lawrence Russell	NGRID	Head of Business Security
Simon Thornhill	NGRID	Head of Privacy
Scott Baron	NGRID	Head of Security Risk & Governance
Paul Dorey	NGRID	Consultant – Ex Chief Security Officer at BP
David Pym	UNIABDN (University College London)	Head of Cyber Security Research at National Grid