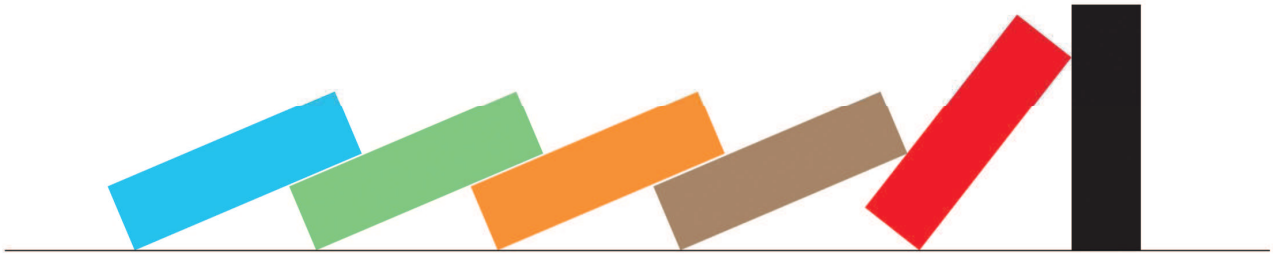

SECONOMICS

D2.2 – National Grid Requirements, First version

R. Ruprai (NGRID), J. Williams (UNIABDN)

Document Number	D2.2
Document Title	National Grid Requirements First Version
Version	1.0
Status	Final
Work Package	WP 2
Deliverable Type	Report
Contractual Date of Delivery	31.07.2012
Actual Date of Delivery	03.08.2012
Responsible Unit	NGRID
Contributors	UNIABDN, NGRID
Keyword List	CNI
Dissemination level	RE

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: Prof. Julian Williams julian.williams@abdn.ac.uk
6	TMB Transports Metropolitans de Barcelona	FERROCARRIL METROPOLITA DE BARCELONA SA, Carrer 60 Zona Franca, 21-23, 08040, Barcelona, Spain http://www.tmb.cat/ca/home	Contact: Michael Pellot mpellot@tmb.cat
7	Atos	ATOS ORIGIN SOCIEDAD ANONIMA ESPANOLA, Calle Albarracin, 25, 28037, Madrid, Spain http://es.atos.net/es-es/	Contact: Silvia Castellvi Catala silvia.castellvi@atosresearch.eu
8	SECURENOK	SECURE-NOK AS, Professor Olav Hanssensvei, 7A, 4021, Stavanger , Norway Postadress: P.O. Box 8034, 4068, Stavanger, Norway http://www.securenok.com/	Contact: Siv Houmb sivhoumb@securenok.com
9	SOÚ Institute of Sociology AS CR	INSTITUTE OF SOCIOLOGY OF THE ACADEMY OF SCIENCES OF THE CZECH REPUBLIC PUBLIC RESEARCH INSTITUTION, Jilska 1, 11000, Praha 1, Czech Republic http://www.soc.cas.cz/	Contact: Dr Zdenka Mansfeldová zdenka.mansfeldova@soc.cas.cz
10	nationalgrid THE POWER OF ACTION	NATIONAL GRID ELECTRICITY TRANSMISSION PLC, The Strand, 1-3, WC2N 5EH, London, United Kingdom	Contact: Dr 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

Document change record

Version	Date	Status	Author (Unit)	Description
0.1	06/07/2012	Draft	R.Ruprai (NGRID), J.Williams (UNIABDN)	Initial Draft
0.2	09/07/2012	Draft	R.Ruprai (NGRID), J.Williams (UNIABDN)	Minor changes and amendments following internal comments
0.3	12/07/2012	Draft	R.Ruprai (NGRID), J.Williams (UNIABDN)	Changes and amendments following comments by National Grid CISO
0.4	13/07/2012	Draft	R.Ruprai (NGRID), J.Williams (UNIABDN)	Approval of document by National Grid CISO for quality and consistency checks against other Work Packages
0.5	16/07/2012	Draft	E. Chiarani (UNITN)	Quality check completed. Some minor changes requested
0.6	17/07/2012	Draft	R.Ruprai (NGRID), J.Williams (UNIABDN)	Further minor changes following quality check
0.7	27/07/2012	Draft	R.Ruprai (NGRID), J.Williams (UNIABDN)	Final minor changes following internal quality and consistency check
0.8	03/08/2012	Draft	Fabio Massacci (UNITN)	Final check by Seconomics Project Co-ordinator
1.0	03/08/2012	Final	R.Ruprai (NGRID), J.Williams (UNIABDN)	Finalised version following review by UNITN for submission to the European Commission

INDEX

Executive summary

This report presents the first version of National Grid's requirements for Electricity Transmission with respect to Work Package 2 of the SECONOMICS project. The report covers how the requirements for this case study will fit into the greater work plan of the SECONOMICS project. In addition it covers a series of case scenarios in the current and future states of the UK electricity transmission which are candidates for the modelling work to be carried out by the RTD work packages (WPs 4, 5, 6).

This report lays the groundwork to answer the following questions in the final version of National Grid's requirements

- Does the current CNI regulation adequately and appropriately ensure that National Grid mitigates the risks in the current state i.e. are the current regulatory frameworks fit for purpose?
- Are the current regulatory frameworks flexible and adaptable enough to manage the future state?
- What regulatory frameworks would be better in the current and future states?

1. Introduction

This is the first version of the requirements and covers a broad menu of potential case study scenarios that will be filtered down and researched in detail in the final requirements document Deliverable 2.3 (D2.3). Sections 1 and 2 outline in more detail the manner in which the document conforms to the wider goals of the SECONOMICS project.

The case study elements of work package 2 are designed to cover the broad area of critical national infrastructure protection through the example of electricity transmission. National Grid (NGRID) is the project partner with the relevant subject matter expertise and experience in this area.

1.1 Scope of report

Work Package 2 (WP2) focuses on the different aspects of security within critical national infrastructure (CNI) including policy, regulation, risk assessing and best practices.

The deliverables within WP2 are listed below:

D2.1 Ethical opinion/authorisation
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 2.2 (D2.2) of WP2. Within the wider context of this work package, this deliverable is the first version of the CNI requirements which will lead to a final and more in-depth requirements assessment and analysis in Deliverable 2.3 (D2.3).

The scope of this deliverable will first be to introduce the CNI case study and National Grid's role and responsibilities as a provider, operate and owner of CNI. The scope will also focus on the key CNI stakeholders and the relationships between them, both governmental and none governmental. A key objective from looking at this will be the potential strategic directions for regulation and cost benefit analyses of implementing different levels/types security. The final report (D2.3) will make recommendations around the strategic direction that CNI security policy should take, to enable CNI assets to be protected at a level commensurate with the preferences of key stakeholders.

1.2 Overview of the document

This document, being the first version of the 'National Grid Requirements', will cover a number of areas that Deliverable 2.3 will look into further. Therefore, this document will set the scene and the context for that further research.

The document is organized as follows:

- Section 2 titled ‘Project objectives and expected outcomes’ will describe the objectives of the SECONOMICS project and WP2. The expected outcomes will be presented, both from the work package and the SECONOMICS project as a whole.
- Section 3 will give a background of the CNI case study in detail. This will provide context for the proceeding sections as well as the other WP2 deliverables.
- Section 4 presents National Grid’s stakeholders at an internal, national and supranational level. An engagement plan will be included showing how we will engage with the stakeholders described to facilitate the aims and expected outcomes of WP2 and the wider project.
- Section 5 provides technical background on the security methodology and frameworks that will be use to describe the security impacts, threats and risks in the security scenarios presented and the subsequent requirements.
- Section 6 then moves forward into the ‘Current’ and ‘Future’ security scenarios relevant to National Grid as an owner and operator of CNI. This report, being the first version of the National Grid Requirements, will not go into the detail of the security impacts, threats and risks of those security scenarios but will instead give context and scope around the scenarios.
- Section 7 introduces two methods for the development of regulatory structures within this area: a rules approach versus a principles approach to regulation, complete with a series of examples. The remainder of the section provides relevant economic models that are related to corporate and public policy in this area as a direction for measuring the appropriateness of the two methods considered.

.

2. Project objectives and expected results

The goal of SECONOMICS is to synthesize sociological, economic and security science into usable, concrete and actionable knowledge for policy makers and social planners responsible for security of the citizens of European countries. The project is driven by industry case studies and will specifically identify security threats to transport (air and urban and super urban metro) and critical national infrastructure. The research focus places social science and political science at the heart of the modelling framework without forgetting the need for technical science. In particular the project seeks to explore the challenges of pan European coordination in security outcomes for transport and critical infrastructure.

The contribution of the project in the wider field of security will be in developing and improving the modelling of security problems in a technological and socio-economic context and then applying state of the art risk assessments and analysis of the social context to develop optimal policies. The outputs are twofold:

- The first is the assessment of the future and emerging threats in the identified areas with rigorous modelling of the optimal mechanisms for mitigation within the policy domain.
- The second, and more crucially, is a generalized policy "toolkit" that will assist decision makers in identifying and reacting coherently (within the appropriate social context) to future and emerging threats that may arrive long after the project has been completed.

Within SECONOMICS there are ten work packages. The first three focus on case studies for air traffic management, CNI and urban public transport respectively. The second three work packages focus on the research and development of security, society, risk, economic and system models. Finally, the last four work packages focus on the consolidation across work packages, community building and project management.

This deliverable sits within Work Package 2 (WP2), the CNI case study. The main objectives of this work package are:

- To assess and catalogue the interactions of security policy on the operation of CNI and the interaction with internal, national and supranational stakeholders/regulators and the wider European public.
- How are various security concerns viewed from within a provider of CNI and from outside by its stakeholders.
- To provide good practice guidance on how to implement security policy for CNI, balance cost and risk and communication of these trade-offs to the relevant stake holders.

To meet these objectives there are a number of deliverables within the CNI case study (WP2). This particular deliverable is the first version of the 'National Grid requirements' and will only cover the scope of the final report at a high level. With this in mind, this deliverable starts to address a number of the objectives above. By looking into a number of narrative security scenarios that affect National Grid as a CNI provider and operator we will see the current regulatory framework of security in action along with its strength

and weaknesses. This will be linked with the stakeholder information and engagement plan provided in Section 4 so that the interactions between National Grid and its stakeholder can be described and documented in more detail. From this we will then be able to better understand the regulatory framework that operates within this industry.

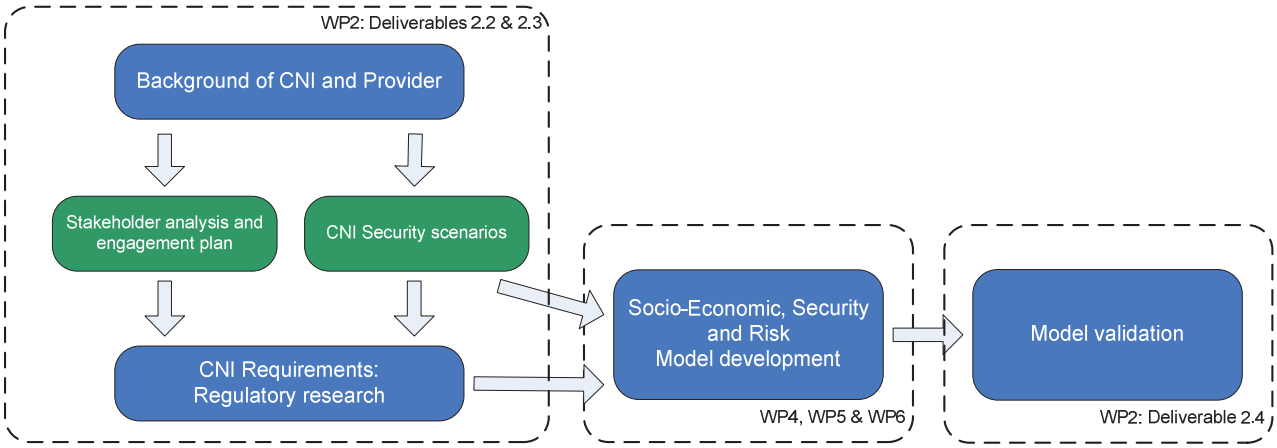

Figure 1 – Approach to the research presented in D2.2 and D2.3

Figure 1 shows diagrammatically how the sections of this deliverable, D2.2, and the final version, Deliverable 2.3 (D2.3), will feed into each other and then to the models produced in work packages 4, 5 and 6. The models produced in these work packages will then be fed back into the industry case studies (Work packages 1, 2 and 3) for validation, as described in Figure 1.

The expected output or result of this deliverable and D2.3 will be as follows:

- a high level view of the threats faced by CNI operators, owners or providers in the areas of electricity transmission
- the potential strategic directions for regulation within CNI
- a cost-benefit analysis of applying regulation to an organisation operating CNI.

The end report will make recommendations around the strategic direction that CNI security policy should take, to enable CNI assets to be protected at a level commensurate with the preferences of key stakeholders.

The expected result of this deliverable and the final report are only part of the expected output or results of the entire work package (WP2). The expect results of the entire work package will be a culmination of the results of this report together with the other deliverables of the work package, Model validation (D2.4) and Evaluation tools for providers and policy paper on future and emerging threats (D2.5). The expected results of the work package are presented below:

- An assessment and cataloguing of the interactions of security policy on the operation of critical national (and supranational) infrastructure and the interaction with national and supranational regulators and the wider European public

- The various security concerns viewed from within a provider of CNI and from outside by its stakeholders
- Good practice guidance on how to implement security policy for CNI, balance cost and risk and communication of these trade-offs to the relevant stake holders.

Both in the expected results of this report and of the work package as a whole, there are references to communicating and engaging with stakeholders. We identify the stakeholders relevant to WP2 in Section 4 of this report and discuss how these stakeholders will be engaged.

3. Case Study Background

National Grid plc is a British multinational electricity and gas utility company whose business activities are in the United Kingdom (UK) and in the North-Eastern United States of America (US).

In the UK, National Grid manages and operates both the electricity and gas transmission networks for the entire country. This includes England, Wales, Scotland and Northern Ireland. National Grid owns the transmission infrastructure for gas and electricity but only in England, Wales and Northern Ireland. In addition, the company owns and operates the distribution of gas in a number of regions of the UK. However, National Grid does not manage the distribution of electricity.

In the UK, National Grid employees approximately 10,000 people working across England and Wales. This includes the 24/7/365 control centres for electricity transmission and gas transmission for the UK.

In the US, the structure of the energy and utilities market is some what different to the UK. As such National Grid own and are responsible for the generation, transmission and distribution of electricity in the following states of the North-Eastern US: upstate New York, Massachusetts, Rhode Island, New Hampshire and Vermont. The company supplies electricity to over 3.4 million end-user customers. For gas, National Grid own and operate gas networks in the following states of the North-Eastern US: upstate New York (including New York City), Massachusetts, Rhode Island, New Hampshire and Vermont. The company delivers gas to approximately 3.5 million customers in these states. National Grid has approximately 18,000 employees across the North-Eastern US.

The focus of National Grid's input into SECONOMICS, and WP2 in particular, will be the UK electricity transmission network, otherwise referred to as 'the grid', in the UK. Whilst the focus of the research will be in the UK there may be potential areas of input from the US such around regulatory frameworks and the threat landscape of electricity transmission.

In this section we will describe how the grid provides and controls electricity transmission across the country.

3.1 Electricity Transmission

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

- Generators of electricity i.e. coal, gas, nuclear, solar, wind (etc.) power stations
- Distributors of electricity (the customers) i.e. those organisations that distribute electricity in a local/regional area
- The 'highway' of high-voltage electrical wiring that connects generators to the distributors
- Tele protection system to safeguard the public when transmission lines are damaged

- The data highway that travels with the power cables which provide voice and data, such as demand, supply, frequency etc., from the generators and distributors
- The Supervisory Control and Data Acquisition (SCADA) systems that take the data feeds and balances the electrical transmission grid through its links to all the generators and distributors.

To understand electricity transmission it is useful to see how the elements above connect with each other in the wider picture. Figure 2, below, shows the full lifecycle of electricity from generation to distributor substation down to residential consumers. This diagram takes into account the elements described above and the scope of National Grid's responsibility is shown in part 'B Transmission'.

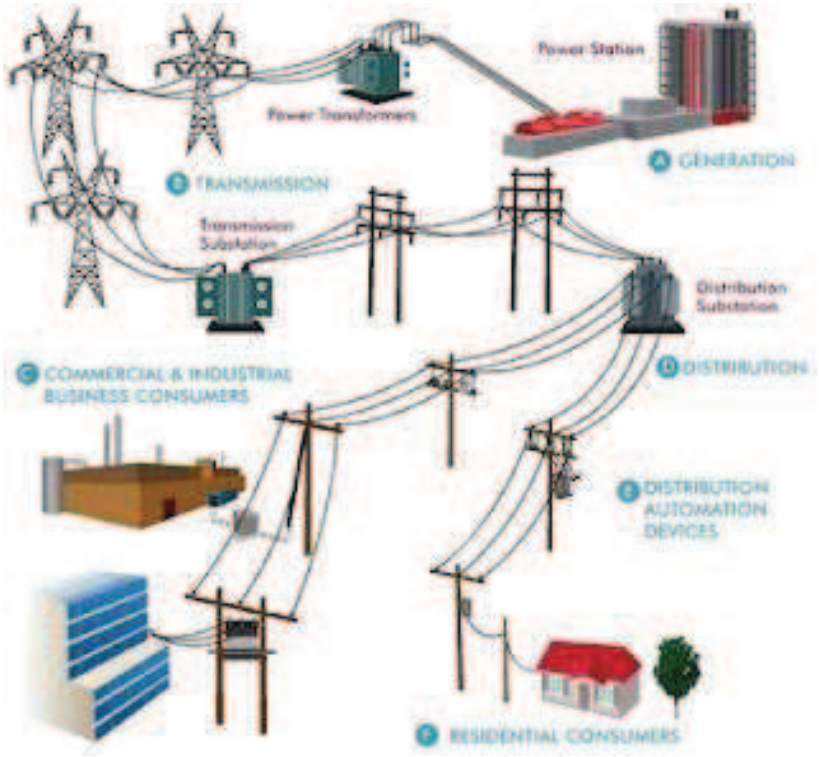

Figure 2 – Complete lifecycle of electricity delivery in the UK

National Grid's role within the wider picture of electricity delivery is to ensure that the demand of electricity by the distributors is met by the supply of electricity by the generation companies. The process for doing this is called 'Balancing' and is explained in more detail in the next subsection.

3.2 Balancing the Electricity Transmission Network

In order to balance the network we first need to understand more about how the electricity transmission control centre and SCADA systems are connected to the grid.

For any specified time period National Grid needs to ensure that supply of electricity is meeting demand. The way in which this is done accurately is to view the frequency of the network. All generators output electricity as alternating current with a frequency of 50Hz. If supply is exactly meeting demand the frequency remains at 50Hz. However, if demand increases this causes extra load to be put on each generator and the frequency at each generator, and thus the entire network, drops. On the other hand if demand falls, the load on each generator drops and the frequency of the network rises. It is the frequency of the network that the control room monitors. If the frequency of the system can be kept within tight limits then the network can be considered balanced. In the UK the acceptable limits of the frequency of the network is between 49.5 Hz and 50.5 Hz.

Figure 3 presents a simplified logical diagram illustrating how the SCADA systems within the control centre are connected to the generators. The measurement and data links enable the control systems to monitor the frequency across the network. The control link with the generators allows the control systems to ramp up or down the electricity output at certain generation sites.

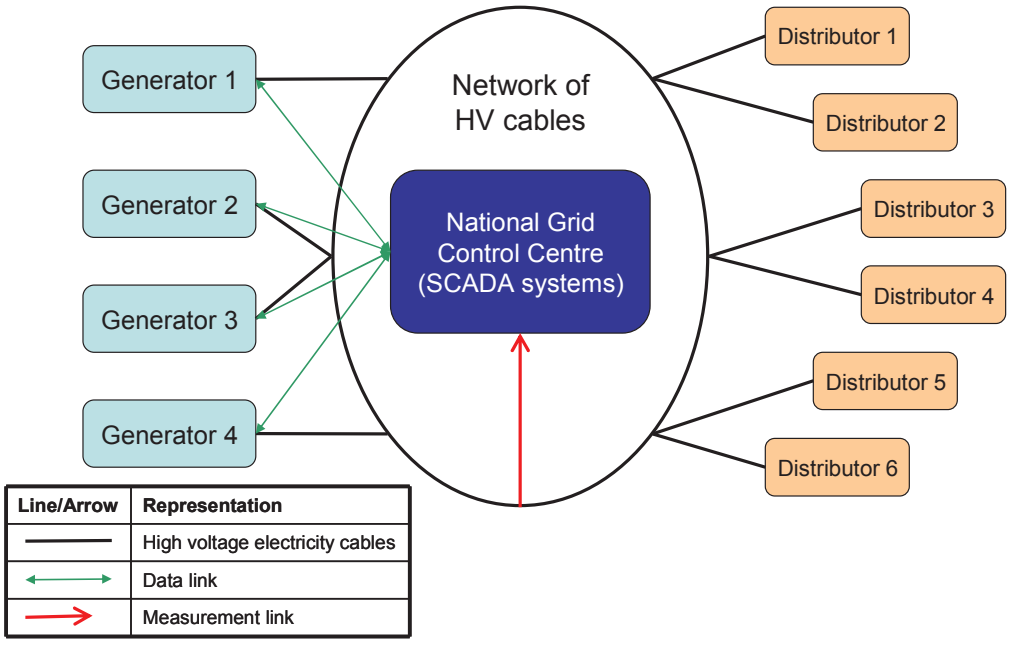

Figure 3 - Simplified logical diagram showing the links between the SCADA control systems and the grid

The frequency control algorithms and mechanisms decide when to increase or decrease the output of electricity at the different generation sites in order to balance the network. For example if frequency of the system starts to fall below 50Hz this shows demand is outstripping supply. Therefore at the pre-determined trigger point the frequency system will ask for increased output from the appropriate generators, which in turn will increase the frequency back to 50Hz.

There are a number of factors that make this process more involved:

- National Grid need to be able to anticipate demand at time periods in the future to forecast how much electricity needs to be generated in advance

- The varying generation sites have different:
    - base loads: the amount of energy that they always produce unless the generation site is turned off
    - electricity output that can be ramped up or down
    - lead times or speed at which the site can increase or decrease electricity output
- National Grid must always have reserve output on standby for unexpected demand increases.

There are numerous other factors that affect the market of wholesale electricity supply in privatised markets such as the one in the UK and across Europe. The issues with such privatised markets as well as other market structures will be discussed in Section 7.

3.3 Previous Incidents

In recent years there have been a number of incidents to electricity transmission grids across the world resulting in power outages to large numbers of people for significant periods of time. A sample of these incidents has been listed below:

- In 2003 there was a major blackout in Italy affecting a total of 56 million people across the country. The blackout was the result of a power line between Switzerland and Italy being damaged causing a cascade effect resulting in other generation sites to trip.
- In August 2003 there was a major blackout in the North-eastern USA and Ontario, Canada affecting an estimated 10 million people in Ontario and 45 million people in the USA. The cause of the outage was a failure by the relevant power company to recognise, understand and manage their systems and protective systems.
- In January 2005 a cyber attack knocked out power to three cities north of Rio De Janeiro, Brazil affecting tens of thousands of people.

In the next deliverable, D2.3 National Grid Requirements Final Version, we will discuss these and other power outages, as they fit into the case study.

4. Stakeholders and engagement plan

During the course of the SECONOMICS project National Grid will engage with a number of stakeholders and stakeholder groups. These stakeholders can be put into the following groups:

- Internal National Grid UK stakeholders: These are teams internal to National Grid in the UK covering electricity transmission
- Internal National Grid US stakeholders: As National Grid owes and operates electricity transmission in the US as well as the UK, we will engage with the internal teams in the US who can provide an important input to this work package
- National stakeholders: Stakeholders in the UK which breakdown further into regulatory organisations, agencies and special interest groups (SIGs)
- Supranational stakeholders: This covers Europe, US and global entities and breaks down further into regulatory organisations, agencies, SIGs and vendors.

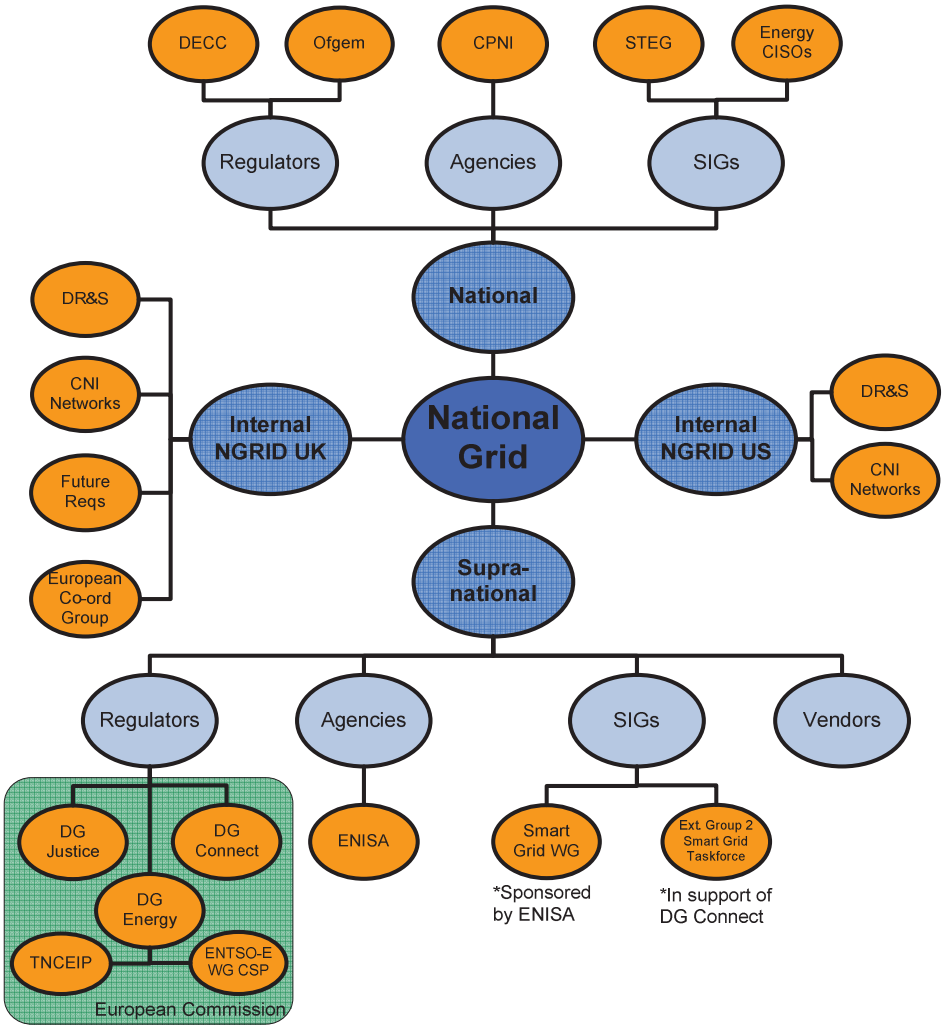

Figure 4A – National Grid Stakeholder Map

Acronym	Full name
DR&S	Digital Risk & Security
DECC	Department for Energy and Climate Change
Ofgem	Office for gas and electricity markets
CPNI	Centre for the Protection of National Infrastructure
STEG	Smart Metering Security Technical Experts Group
Energy CISOs	UK Energy Chief Information Security Officers Round table
DG	Directorate General of the European Commission
TNCEIP	Thematic Network on Critical Energy Infrastructure Protection
ENTSO-E CSP WG	European Network of Transmission System Operators for Electricity Cyber Security Protection Working Group
ENISA	European Network and Information Security Agency

Figure 4B – National Grid Stakeholder acronyms and full names

Figure 4A presents National Grid's stakeholder map for the SECONOMICS project and Figure 4B gives the full names of the acronyms used in the stakeholder map. The map aligns to the groups described above and the leaf nodes of the map (objects in orange) detail the actual stakeholders and stakeholder groups. The detail of the aims of our engagement with the stakeholders is presented in Table 1 below.

Table 1 - Aims of the engagement with stakeholders

Stakeholder		Engagement
Internal NGRID UK	Digital Risk & Security (DR&S)	DR&S in the UK are tasked with managing and mitigating the cyber security risks within National Grid UK through security strategy, governance, risk, compliance, consulting, architecture, threat and incident management. For WP2, we will be in constant engagement with DR&S to understand the current and future security threats and risks to National Grid's business and the current regulatory requirements. In addition, the Chief Information Security Officer (CISO) of National Grid is the main sponsor of the company's involvement in the SECONOMICS project. Therefore it is key that we engage with the CISO to ensure that the requirements, model validation and policy frameworks research are appropriate disseminated and meets the expectation.
	CNI Networks	The CNI networks team in the UK deal with the operations of the electricity transmission network. They are best placed to advise the project on networks and systems that constitute CNI, the regulatory requirements on them, not just in security, and how they meet (or go

		beyond) what is required from the regulation.
	Future Requirements	Future Requirements are a team that look at the future requirements of the electrical transmission network in the short, medium and long term. Through liaising with them we can get their views on what their expectations are of the future requirements. In addition, we may be able to provide some valuable input to these expectations from the output of the SECONOMICS project.
	European Co-ordination Group	Cross-business group in National Grid to establish consistent approach to EU issues. We will engage with this group to understand our approach to current and expected future EU issues.
Internal NGRID US	Digital Risk & Security (DR&S)	DR&S in the US are tasked with managing and mitigating the cyber security risks within National Grid US through security strategy, governance, risk, compliance, consulting, architecture, threat and incident management. Whilst the SECONOMICS project is focussed on regulation and policy at a European level, National Grid's US business can provide some valuable input. In particular, in the US part of the business (including electrical transmission) is regulated by the North American Electric Reliability Corporation (NERC) and there are a number of standards that National Grid must adhere to. One of these sets of standards is the 'Critical Infrastructure Protection' standards otherwise known as NERC-CIP and these heavily influence the company's security strategy, governance and compliance. This regulatory framework will be a key example in Sections 6 and 7 of this report and WP2 as a whole.
	CNI Networks	The CNI Networks team in the US will aid the DR&S team in the US in providing information on National Grid's response to the NERC-CIP standards at both a high level and at the 'coalface'. In addition, the CNI networks team are key to understanding how the different facets of the business are affected by the NERC-CIP regulation. This will be an important input to the discussion on policy and regulatory framework in Section 7.
Nat	Department of Energy & Climate Change (DECC)	DECC is the government department which is charged with the responsibility to manage all aspects of energy

		and climate change in the UK. National Grid has a very important relationship with DECC as this is the government department it reports to with regards to its regulated duties. This includes the managing and operating of the electricity transmission grid and its balancing. We will engage with DECC with the following aims: • Gain clarity on the current regulatory frameworks • Understand how security investment is included in the pricing and charging models • Identify who defines requirements that National Grid have to meet in information/cyber security • Hope to engage DECC on different policy frameworks that could apply to CNI operators such as National Grid from the outputs of the SECONOMICS project.
	Office for gas and electricity markets (Ofgem)	Ofgem are a quasi-governmental organisation that regulates the market of demand and supply of electricity and gas in the UK. They are acutely linked to DECC and many of the engagement aims with Ofgem are those given for DECC.
	Centre for the Protection of National Infrastructure (CPNI)	CPNI is a UK government agency, which is part of the intelligence services, whose duty it is to ensure that all aspects of critical national infrastructure in the UK are protected. This includes, but is not limited, to the availability, physical security, information security and reputation are protected. As National Grid own and operate CNI, CPNI provides guidance and advice on many of these aspects of security. CPNI are well placed to provide a view on the current and future states of security of electricity transmission as well as provide input on the current threat landscape. In addition we hope to engage with CPNI on their views of different regulatory frameworks and share with them the output of the SECONOMICS project.
	Smart Metering Security Technical Experts Group (STEG) sponsored by DECC.	The UK government are currently progressing a programme of rolling out smart meters across the country. There is a significant security element to this programme and STEG is a group which DECC operate to share views and ideas on security with the energy industry in the UK. National Grid are a member of this group and we aim to utilise this membership to understand the threat and risk landscape in the energy

		market and how smart metering affects electricity transmission focussing on security.
	Energy CISO Round table	National Grid's Chief Information Security Officer is a lead member of the Energy CISO Round Table whose membership includes CISOs of other energy companies (suppliers and distributors) in the UK. This forum provides us the opportunity to gain insight to the current security posture of the energy industry as a whole and share ideas relevant to policy, in this industry, at a board level.
Supranational	Regulators including • DG Justice • DG Connect • DG Energy	The regulator at the European level is the European Commission which consists of a number of Directorate Generals (DGs) with a variety of remits. Three DGs which we may engage with have been listed, including: • DG Justice which covers justice, fundamental rights and citizenship policies across Europe • DG Connect manages the digital agenda of the EU focusing on communication networks, content and technology. ENISA is an agency which reports to this DG and it is through this agency that we will engage (see below) • DG Energy manages all areas of strategy, legislation, enforcement etc. for the energy industry across Europe. We will engage with this DG through two groups, TNCEIP and ENTSO-E, and this engagement is described below. Our key objective from this project is to advise the European regulator on policy frameworks for this industry and we aim to do this through the groups described below.
	Thematic Network on Critical Energy Infrastructure Protection (TNCEIP)	TNCEIP are a network established by DG Energy to bring together operators of critical infrastructure in energy across Europe. This group addresses topics such as threat assessment, risk management and cyber security in the area of critical infrastructure for energy. Through engaging with TNECIP we aim to: • Understand what the regulators see as the main drivers for regulation in the CNI industries including electricity transmission. • Understand what issues go beyond sovereignty and subsidiariety of an individual national state.

	European Network of Transmission system Operators for Electricity (ENTSO-E) Cyber Security Protection (CSP) WG	ENTSO-E is a group which brings together all the electricity transmission operators across Europe, National Grid included. It provides a forum for the transmission operators to discuss ideas, progress and changes in different areas of the industry. There is a specific Cyber Security Protection working group of ENTSO-E where cyber security issues are presented and discussed, which National Grid chairs. This working group, and ENTSO-E as a whole, are an important stakeholder for WP2. In the CSP WG we aim to get views and input on regulation, risks and threats to electricity transmission. We endeavour to inform the group about the SECONOMICS projects with a view to share the policy frameworks deliverables with them. The driver for this is to foster a better understanding of the advantages and disadvantages of different regulatory frameworks of the industry across Europe.
	European Network and Information Security Agency (ENISA)	ENISA is an agency of the European commission with a focus on information security. To this end we will engage ENISA to understand their work programme in the space of CNI and electricity transmission with an aim to advise on what work programmes may be required in the future in this area.
	Smart Grid WG sponsored by ENISA	This SIG is a working group on Smart Grids sponsored by ENISA. We will engage with the group to understand the economic drivers and inhibitors for Smart Grids and then to understand the risks involved to energy delivery (transmission included) as a whole.
	Expert Group 2 for the Smart Grid Taskforce	This is another working group on Smart Grids that we aim to engage with to gain views on the direction of the European Commission on Smart Grids.
	Vendors	We aim to engage with vendors (specifically SCADA systems providers) by attending relevant events and conferences globally.

5. Security Methodologies and Frameworks

National Grid is a large organisation whose safe and secure operation is essential for the delivery of electricity and gas to citizens in both the US and UK. Due to the criticality of the electricity SCADA systems and networks for the safe and consistent delivery of electricity to end users understanding the potential security threats, risks and impact to the system is paramount.

In addition, it is through this better understanding that we can appreciate how different regulatory frameworks and security policy interact and affect the operation of CNI. This will be discussed in Section 7.

In the wider information security arena there are a number of risk assessment methodologies which we could utilise here to assess levels of impact, threat and risk. For example:

- IRAM: Information Risk Analysis Methodology by the Information Security Forum
- FIRM: Fundamental Information Risk Management by the Information Security Forum
- CRAMM: CCTA Risk Analysis and Management Methodology by the Central Computing and Telecommunications Agency (CCTA).

A downside of a number of these methodologies is that they do not have an appropriate framework in place to measure risk to CNI. The reason for this is that many risk assessment methodologies focus on information security risks to an organisation such as financial, reputational and operational risks. However, CNI providers and operators have the capacity and capability to impact a region or country's infrastructure and citizens. Therefore, any risk methodology used needs to be able to measure impact to the individual organisation, the wider industry and economy, citizens and the country as a whole.

In the UK, the risk assessment methodology used by government departments is specifically focused on IT systems and supporting processes which have the potential to impact the country's infrastructure, economy, international relations, defence, public services and public safety. The methodology can measure impact to an individual organisation all the way up to impacts that affect the entire country and its citizens and thus appropriate risks can be identified. The risk assessment methodology and process is described in detail in HMG Information Assurance Standard No. 1[1]. This document is also referred to as 'IS1'. IS1 applies the same methodology of assessing risk to the three attributes of information security namely confidentiality, integrity and availability.

We will aim to use IS1 in conjunction with other well known risk assessment methodologies to assess the level of threat and risk within the case study.

[1] HMG Information Assurance Standard No. 1 – Technical Risk Assessment v3.51 by CESG – The National Technical Authority for Information Assurance and the Cabinet Office

At the highest level the risk of an unwanted event happening is a product of the likelihood that the event will happen and impact of the event happening (R = L x I). So, going to the next level of detail one needs to look at the likelihood and impacts to determine risk. In the next two subsections we will discuss impact and likelihood.

5.1 Impact

First we will discuss the impact of incidents. To measure and compare levels of impact IS1 provides Business Impact Level (BIL) tables[2]. The BIL tables provide a break down of the different areas of impact, such as public safety, economy etc., and provides metrics against compromises in confidentiality, integrity and availability of information and ICT systems. The business impact level scale ranges for 0 (no impact) to 6 (extreme impact).

A number of tables are provided for different industry sectors within a country. One of these industry sectors includes CNI but there are other impact aspects which should be considered. Therefore a summary table of sub-categories relevant to a provider and operator of CNI can be found in Appendix 1.

5.2 Likelihood

In IS1, likelihood is broken down further. The likelihood that an event can happen is the likelihood that a threat agent can exploit vulnerabilities in the asset. Whilst vulnerabilities are different across different organisation's assets the threat agents can be similar so it is important here to focus on threat.

IS1 provides a very clear and granular process for determining level of threat. In IS1, the level of threat or 'threat level' is a product of the threat actor's capability and motivation. The scale of a threat actor's capability ranges from 1 (very little) to 5 (formidable) and a detailed table containing descriptions of the different levels can be found in IS1 and has been reproduced in Appendix 2. The scale of a threat actor's motivation ranges from 1 (very low – indifferent) to 5 (very high – focused) and a detailed table containing descriptions of the different levels can be found in IS1 and has been reproduced (with minor changes) in Appendix 2.

The threat level posed by a threat actor is then a product of these two and a metric table of threat levels has been produced in IS1 and is also given in Appendix 2. These threat levels can apply to both a malicious attack and accidental incident. However, it is viewed by IS1 that an accidental incident cannot pose a 'Critical' level of threat. For the electrical transmission network being CNI we have not ruled out the possibility of a 'Critical' accidental threat.

5.3 Risk

Given the business impact and threat levels identified above, IS1 determines the levels of risk as a product of these, using a metric table which can be found in Appendix 2. Therefore instead of Risk being the product of Impact and Likelihood, Risk is now a product of Impact and Threat Level.

[2] BIL tables within HMG Information Assurance Standard No. 1 – Technical Risk Assessment v3.51

However, once one has determined business impact and the level of threat the determination of a risk level is not an automated process. For a particular scope, a risk assessor has to complete the following steps before a risk level can be determined:

- Decide the type of threat actor that will be attacking the systems from a pre-determined list within IS1
- Understand the most influencing threat source where the threat level has been determined using the process above
- Identify the different methods of compromise that the threat actor could exploit and the associated threat level for each.

Once this list has been completed and the associated threat level and impact have been assigned the risk level will be determined for this using the table above.

We will use the methodology described above to discuss the different aspects of the CNI case study.

6. CNI Security Scenarios

To better understand the security threats, risks and impacts to National Grid and the UK as a result of a breach we will discuss two different states of National Grid's business that is relevant to CNI. The first will be the 'Current' state which considers the security threats, risks and impact to National Grid's current CNI systems, processes and assets. The second will be the 'Future' state. This state is less clear as it considers the security threats, risks and impacts to National Grid's future CNI systems, processes and assets. These future systems, processes and assets are not certain but represent National Grid's view of what it expects to see in the future.

In this report, D2.2 National Grid Requirements First Version, we will begin to look at the security impacts, threats and risks but these will be covered in more detail in the final report, D2.3 National Grid Requirements Final Version. Implicitly included in each aspect of the current and future states are relevant physical security facets and how they interact with the digital or cyber security facets. These will also be covered in more detail in the final report, D2.3.

6.1 Current State

As we have seen in Section 3 there are many aspects to National Grid's CNI systems, processes and assets. The systems and assets will have different impacts to the business, UK citizens, UK infrastructure and economy, if they were to be compromised whether accidentally or maliciously.

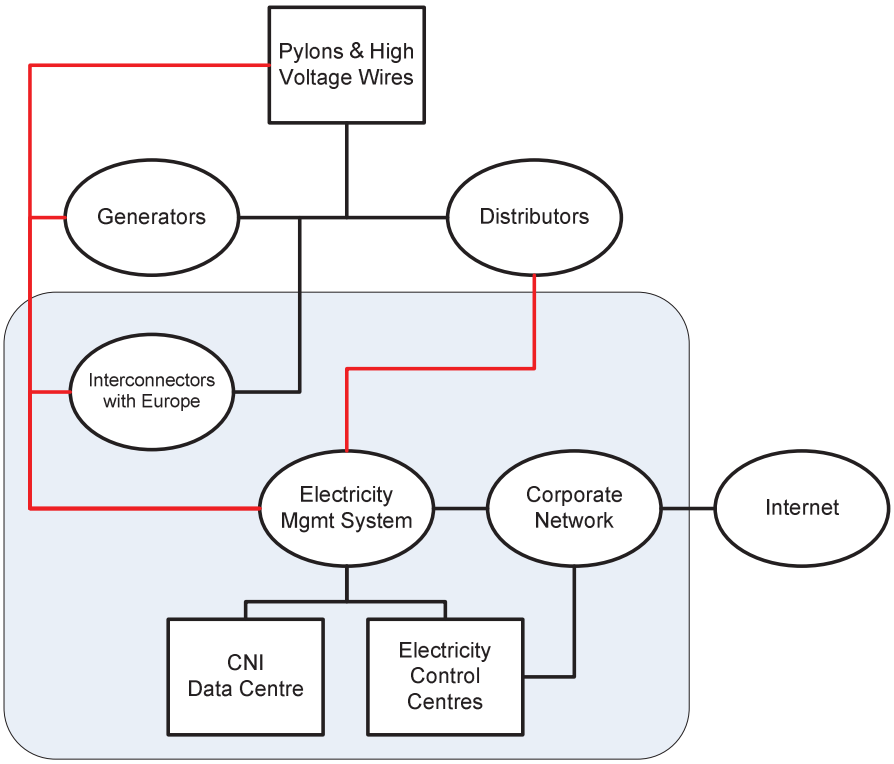

Figure 5 - Logical diagram

Figure 5 gives a logical view of the different parts of the electricity transmission grid that National Grid operates. The diagram brings together the different parts of the infrastructure as well identify which parts are in scope. The oval objects represent the business objects and the rectangular objects represent the support objects that support the business. The links between the objects represent either:

- Business to business object links showing a data, physical and dependency link
- Support links between business objects and support objects
- Data links between business objects (shown in red) such as the one between the generators and the Electricity Management System.

The grey area represents the scope of this case study within SECONOMICS. This diagram follows the framework laid out in HMG IS1[3] for the risk assessment diagrams and allows us to understand the interdependency of the objects as well start the process of identifying the impact if a particular object was compromised either accidentally or maliciously.

A number of the objects in Figure 5 have been described in the Case Study Background in Section 3. However, there are a number of objects and aspects to Figure 5 that we will discuss in more detail here as well as begin to look at the security impact, threats and risks.

6.1.1 Interconnectors

The 'Interconnectors' business object refers to the energy interconnectors connecting the UK to France and the Netherlands.

The different countries across Europe (including the UK) have separate electricity grids. Over recent decades as electricity usage has increased there has been a need for the countries across Europe to utilise electricity from its neighbours in order to meet demand. Making this functionality possible allows countries to limit the amount of reserve capacity it must hold as well as help with any potential shocks in demand or supply such as increases in demand due to large events or unexpected malfunctions at power generation sites.

To make this a possibility, interconnectors were built between neighbouring electricity grids which allow for the potential of electricity to flow between countries. Many interconnectors have been built across Europe and central European countries such as Switzerland have interconnectors with all its neighbours. Each individual country's grid operator needs to balance their respective grids. However, there is the added complexity that they need to meet demand or supply of electricity from the interconnectors.

In order for the grid to understand the requirements at the interconnectors at any specific time a data link is needed between the SCADA control systems and the interconnectors. This highway of data links at interconnectors is referred to as the 'Electronic Highway'.

[3] HMG Information Assurance Standard No. 1 – Technical Risk Assessment v3.51

The UK has two interconnectors which are often used to import electricity rather than export. Whilst the interconnectors are used there is not a reliance on them to meet demand and thus the impact of not having the interconnectors available for a short of medium length of time would be low. On the other hand, for other European countries that rely on electricity imported across their interconnectors, the impact of the interconnector not being operational will be higher.

6.1.2 The Electricity Management System and Data links with Generators, Distributors and Interconnectors

As described in the Case study background, Section 3, the Electricity Management Systems requires information from the electricity generators, the distributors, the interconnectors and throughout the physical assets across the grid in order to balance the system. This data may include:

- Frequency information
- Current levels of energy flow
- Capacity information.

This information is critical for the correct balancing of the grid.

In many cases the data links are reliant on people to perform actions dependent on what the data is indicating. For example, if demand is increasing and thus frequency of the grid falls, by looking at the capacity of generation sites an operator can decide which generation site(s) can be ramped on or switched on. Some of these operations are automated but currently this process still requires human intervention in order to balance the grid.

It is important to consider the attributes of information security (confidentiality, availability and integrity) and their priority with regards to CNI. Within the electricity transmission network a breach in confidentiality has a much lower impact to maintaining supply, compared to a breach in availability or integrity of information. Intuitively, the availability of information within CNI is viewed as having a high impact on the operational effectiveness; however, with increased reliance on automation, integrity is now just as critical and potentially presents a higher impact on managing CNI. For example if the real-time information flowing across the data links was not available to the Electricity Management System then balancing the network would become very difficult. However, the integrity of this data seems the most important. This is because if the data becomes unavailable to the system and operator, this will be clear from the outset of the problem. Alternatively, if no or weak integrity protection is applied, the system and the operator will not be able to identify whether the information has been changed. An attacker can then change the data to the detriment of the system as a whole.

For example, if the data is showing that the frequency of the grid is falling below the desired 50Hz and an attacker can manipulate the data to show that it is instead rising, this will result in the operator ramping down / or switching off sites. Thus, this will cause the frequency of the grid to drop further and will start the ‘tripping’ of generation sites as occurred in Italy in 2003 (see Section 3.3). This shows that integrity protection

of the data travelling across these data links is very important to the safe and secure operation of the grid.

6.1.3 Corporate Network and IT infrastructure

National Grid relies on a large and complex IT estate and infrastructure to deliver its business objectives. As the electrical generation industry evolves and the economic and regulatory drivers change, the way the company approaches IT infrastructure, applications and networks needs to adapt. This situation is influenced and guided by the need to ensure information security across the company and that appropriate policies, measures and processes are in place. Due to the nature of National Grid's business and that they have been identified as a provider of CNI, an additional dimension has to be considered when developing and implementing the corporate IT architecture.

Current government guidelines mandate additional physical and information security measures be implemented to ensure the protection of the CNI over and above standard IT infrastructure.

The IT systems supporting electric transmission business fall into three functional areas:

- Electricity Transmission (telemetry and management (primarily SCADA systems);
- Electricity Balancing (the interaction between the grid and the generators and distributors);
- Business Systems (the business support systems SAP, Internet, etc.)

The challenge for the grid operator is to securely interconnect the first two areas which are designated as CNI, to the business area.

SCADA systems are traditionally mature and physically separated from other IT. However, business drivers to automate processes have led to an increased reliance on network technologies to collect the SCADA information. Business systems however, are now becoming more reliant on the internet and electronic information exchanges between the transmission network provider and its customers.

There are both business and operational dependencies today to exchange information between the CNI (SCADA) type systems and business systems or other operators SCADA systems, this is creating a new dynamic on information security, with respect to increased threats vectors and potential impact, if a breach of security occurs.

6.1.4 Employee Behaviour

All of the business and support objects in Figure 5 have a people aspect to them. In particular, it is the employees of the CNI operator that can affect the level of threat, impact and risk to those objects.

Employee behaviour which is misaligned to the organisation can have significant effects on them any organisations. Across different organisations the motivation of employees, both careless or malicious are similar, although for an operator of CNI, the impact of an incident can be much larger than an organisation that is not an operator of CNI.

In a generic organisation with IT systems one can group employees as normal users and privileged users. These two groups of users have different levels of access and rights to

the IT infrastructure thus the impact of a privileged user compromising the IT system will be higher than a normal user. Another way in which this can be viewed is that a privileged user has a greater capability to compromise the system versus a normal user.

Employees, both privileged and normal, can be put into one of four groups. These groups have different threat levels associated with them. In Table 2 below we give an estimation of the threat level posed by these groups of employees. In the final version of the report (D2.3) we will give a more accurate assessment based on more detailed background information.

Table 2 - Threat level posed by employees

Employee Group	Description	Normal User Threat Level	Privileged User Threat Level
Care-less & routine	Day-to-day violation of information security policies due to ineffective policies or lack of awareness	Negligible	Low
Care-less & business critical	In order to meet business critical needs the information security policies are circumvented	Negligible	Low
Rogue & disgruntled	An employee who was previously a good employee but has since turned rogue due to an event such as being fired, made redundant, change in personal circumstances	Moderate	Substantial
Rogue	A completely rogue employee whose motivation to attack the CNI provider is based on a more sinister reason such as foreign intelligence backing, blackmail, bribery etc.	Substantial	Severe

6.2 Future State

In Section 6.1 we described and discussed different aspects of the security of the CNI Case Study at the current time. We have started the discussion on the security impacts, threats and risks which will be expanded further in the final version (D2.3) of this report.

In order to assess the possible future and emerging threats in CNI, particularly electricity transmission, we need to first start to develop a view of what the future state of electricity transmission will look like. To that end, we will look at the four aspects of the case study described in Section 6.1 and put some initial thoughts together of what the future state may look like. These are given below:

- Interconnectors/Pan-European 'Electronic Highway': Currently, the Electronic Highway allows the sharing of data between the countries on each side of the interconnectors. In the future this may expand to allow commands to flow across the data links allowing systems to automatically decide whether power is ramped up/down across an interconnector by following pre-determined algorithms. For example if country A's and B's grids are connected and country A can send a command to the grid of country B to increase power across the interconnector automatically what does this require in order to be secure? Country B would need to be confident in the security of country A's networks. Some key questions from this would be:
    - As the system becomes more intelligent and automated how does National Grid ensure that it is resilient against cascade effects?
    - How much automation is sensible/practical or achievable?
    - Is the current regulation at a national or European level suitable to deal with this situation? If not, is regulation the best way forward and how can the European regulators maximise the effect of their input?
- The Electricity Management System and Data links with Generators, Distributors and Interconnectors: Looking at a national level, data links between the SCADA systems and generators/distributors may become 'command and data' links in a similar way to the Electronic Highway. Organisations, such as the distributors, will be reliant upon the security of National Grid's system in order to trust commands. This would suggest that a regulatory framework will be needed to assure the standard of security at National Grid. The questions to fall out of this will be similar to that of the Electronic Highway but on a national rather than European level. Also, with the introduction of smart metering across Europe, including the UK, how will this change the threat and risk landscape to National Grid as a transmission operator? How can the country and Europe as a whole be sure that transmission operators are taking the necessary steps to secure their systems as smart metering and then smart grids are rolled out at the distribution level?
- Corporate Network and IT Infrastructure: As electricity grids become more complex, National Grid's business may require more extensive links between the corporate network and the CNI SCADA systems. This may result in more interfaces between the CNI SCADA systems and the internet which would need to be secured. Therefore, what approaches are there from a technical or regulatory view point to deal with this situation?
- Employee Behaviour: It is not clear at this stage how current policy aids National Grid in mitigating the threats and risks posed by employees. Would regulation/ policy hinder National Grid's ability to mitigate these threats and risks? Separately, as the transmission grid becomes smarter the role of employees within the organisation will change. How will the organisation cope with these changes and how will policy and regulation stay in tune with the changing landscape and business requirements?

We can see from the initial thoughts in these aspects of the case study, that there are a number of areas relating to regulation that the final version of the report (D2.3) will focus on. These are presented in the next section along with a background to regulatory frameworks. This will enable us to look at these areas in more detail in the final version of the report, D2.3.

7. Requirements

In Section 6 we began to look at different security aspects of the current and future states of National Grid's electricity transmission operations. National Grid as an owner and operator of CNI needs to adhere to certain regulation in the UK and US. In this section we will start to discuss these regulatory structures and assess them for their appropriateness. The key questions that we will start to look at in this report and will aim to answer in the final version of this report (D2.3) are as follows:

There is some regulation that is imposed on National Grid, in the UK, as an owner and operator of CNI. In addition

- Does the current CNI regulation adequately and appropriately ensure that National Grid mitigates the risks in the current state i.e. are the current regulatory frameworks fit for purpose?
- As National Grid and the energy industry across Europe moves towards the future state, are the current regulatory frameworks flexible and adaptable enough to manage these changes?
- What regulatory frameworks would be better in the current and future states? And can we look at examples elsewhere in the world or in other industries?

In order to answer these questions we will need to look at a number of areas which are broken down into the following sections:

- Section 7.1 looks at the two different high-level approaches to regulation applying to organisations operating critical infrastructure
- Section 7.2 begins to look at how we can assess the usefulness and efficiency of the different regulatory frameworks
- Section 7.3 then carries the discussion from the previous section on to incentives and how they can be modelled in the different type of regulation which will provide a base for the next section
- Section 7.4 will then look at the role of public policy in attempting to create or erode the incentives described in the previous section to effectively manage risks.

7.1 Rules versus Principles and Risk based approaches

Rules are sets of instructions with either a dichotomous (adhered to or not adhered to) or continuous compliance measure (example: 90% versus 50% compliance). Principles are designed to be general statements that define a goal or objective of the entity 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 principle.

The main advantage of principles or risk based approaches to regulation is that they cover a wider range of scenarios than rules based approaches. However, principles devolve discretion to the entity and require guidance on the level of conservatism to be applied to their implementation. On the other hand, a rules based regulatory system

ensures that all parties that need to adhere to it are applying the same set of security controls and can even be onerous as to specify how the controls are implemented. This can be seen as a 'double-edged' sword since all parties will have the same level of security, if there is a gap in the regulation e.g. a particular aspect of security is missed, this will affect all parties in the same way and the *systematic risk* will be high. Alternatively a risk based system, where the individual parties identify the type of security controls that they will implement separately, ensures that the systematic risk is lower.

It is important to note here that the risk based methodology and framework described in Section 5 is simply a particular risk assessment methodology. Both a risk based and rules based regulatory framework could require a risk assessment to be completed but the specific requirements around how it is done and applied to the business are likely to be different.

In the final version of this report we will discuss the current regulation in the UK that National Grid must adhere to for its CNI assets. However, in the next section we discuss the US regulatory framework that applies to National Grid's CNI assets in the US which is a rules based framework.

7.1.1 A Rules based example in the Energy Industry

The North American Electric Reliability Corporation (NERC) is an independent organisation that provides rules and protocols for electricity transmission operators in North America. 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).

NERC Critical Infrastructure Protection (CIP) reliability standards provide rules for power distribution providers on securing critical infrastructure. There are a number of standards documents within the current version which are as follows:

- CIP-001-2a: Sabotage Reporting
- CIP-002-3(a): Cyber Security – Critical Cyber Asset Identification
- CIP-003-3: Cyber Security – Security Management Controls
- CIP-004-3: Cyber Security – Personnel & Training
- CIP-005-3a: Cyber Security – Electronic Security Perimeter(s)
- CIP-006-3c/d: Cyber Security – Physical Security of Critical Cyber Assets
- CIP-007-3: Cyber Security – Systems Security Management
- CIP-008-3: Cyber Security – Incident Reporting and Response Planning
- CIP-009-3: Cyber Security – Recovery Plans for Critical Cyber Assets.

National Grid must adhere to a number of the NERC CIP standards for its CNI assets in the US. In the final version of this report (D2.3) we will look at these standards into more detail as the most appropriate example of a rules based approach in the CNI

electricity transmission industry. In addition we will look at the effects it has on National Grid as an organisation and further afield.

However, as an example we will look at a particular requirement within one of the NERC CIP standards and the possible effects it can have on an organisation.

Asset Identification Rules example

In the NERC CIP standard CIP-002-4a[4] called Cyber Security – Critical Cyber Asset Identification (see Appendix 4), being the newer version of CIP-002-3a, requirement R1 states:

"Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in CIP-002-4 Attachment 1 - Critical Asset Criteria. The Responsible Entity shall update this list as necessary, and review it at least annually."

Attachment 1 of CIP-002-4a then presents a list of 17 criteria for assets to be classified and catalogued as critical assets. These are listed as "*considered Critical Assets*" page 6:1. The interesting contradiction here is that the Attachment 1 list suggests that discretion be applied to the selection of assets (i.e. assets similar to the seventeen listed). However the requirement states that the entity will apply the criteria contained in the attachment. In the rules based approach assets that fall outside this criterion are now outside the critical asset classification for the year in question.

A Principles or Risk Based Alternative

Below we present a principles or risk based alternative to the example above that would better ensure that organisations meet the intended aim of the requirement.

Objective: To ensure that all assets that could lead to (for instance) BIL5 or above incidents be classified and listed. The list is an outcome i.e. all assets that come under this criteria are listed and the list is updated as new assets fall under the criteria rather than at specific annual snapshots.

Examples of critical assets are listed in the Attachment 1, but may not be exclusive to Attachment 1.

7.2 Assessing Efficacy

In order to assess the adequacy of rules versus principles based systems we will need to place in context the incentive structures of the various agents within a system.

For the remainder of this discussion we will focus on the following hierarchy: A public policy maker or regulator setting up a regulatory mechanism for a set of firms in an economy, one of which is a CNI provider (a monopolist in their own market, but critical to the production function of the rest of the economy) each one having a firm specific policy maker and a set of employees for each firm that need to be coordinated. The regulatory mechanisms and policies are focussed on security as this is the domain of

[4] NERC CIP Standard 002-4a Cyber Security - Critical Cyber Asset Identification

interest. There are other elements to this system, which we will consider later on (e.g. insurance companies and attackers generating risks).

At the firm level in this economic system there is a principal (the firm security manager) and a set of agents (the employees carrying out tasks under supervision). We can think of the firm as adjusting a cost-benefit curve relating risks to investments. In Section (7.3.2) we shall make specific assumptions as to the relationship between investment, however at this juncture we only require that the firm can identify a specific level of tolerable risk given a level of investment, assuming that even with investment tending to infinity a finite risk remains (residual risk).

Policy makers weigh the relative importance of each firm in the economic system. These weights need not be equal (although in economics for demonstrative purposes weights are often assumed to be equal to ensure that they are exogenous and the model generalisable). For practical purposes the importance of the security of individual elements of a system maybe more heavily weighted to one company. CNI providers are a useful example of this overweighting. The policy maker then sets out constraints for the various firms in the market to ensure global welfare is maximised. In our system we address two mechanisms for policy implementation, the aforementioned rules approach versus a principles approach.

A generalisation from the economics literature is that alignment of incentives tends to favour principles based approaches (i.e. aligning risk preferences and the inter-temporal substitution between short and long run risks via discount rates). However, this is not always the case. For situations whereby incentives cannot be, or are too difficult to be, aligned, contractual requirements with dichotomous adherence are sometimes favoured.

In the following sections we will begin by providing an overview of the incentive issues within firms and move onto the public good issue of incentives between firms. We shall bring into the discussion aspects of the level at which behavioural restrictions need to be enforced contractually and potential regulatory frameworks and policy mechanisms that affect the evolution of these arrangements.

7.3 Modeling Incentives Principal-Agent Approaches

If we assume that employees need to adhere to certain behavioural constraints to operate towards a firm's specific cost-risk target, and then a natural issue of aligning incentives appears, this is a standard principal-agent problem in economics. As we add up the choices of all of the firms as collections of principals and agents, we now move to a public policy aspect of economics.

A natural question is where to place the specific constraints on behaviour and what mechanism (regulatory framework) should be used to enforce those constraints. In a principles based system a set of idealised outcomes is specified. Alternatively, if a public policy maker sets a series of rules then these rules may: a) conflict with the risk targets of the firms and b) conflict with the target risk of the agents working in the firm. Setting a penalty structure based on violations of rules does not always result in the correct internalisation of externalities at both the level of the firm or the wider economy.

This section will look at firm specific and public policy approaches to managing risk in the following context:

- Principal agent problems within firms and organisations
- Investments in security protection
- Public policy and regulatory approaches (from an economic standpoint)
- The potential role for insurance as a mechanism of regulation
- The potential role of derivatives markets in hedging security risk.

The section is designed to be a general overview and not specifically attached to CNI issues, although examples from this domain are given herein.

7.3.1 Principal-Agent Problems in Risk Management

We can treat part of CNI as an information processing ecosystem, where security leaks have a variety of costs associated with them. Information ecosystems, are commonly characterised by service individuals and organisations (agents) acting on behalf of other user individuals and organisations (principals).

In the CNI industry as with other industries there are two levels to this. The policy maker or regulator at the very top (principal) communicates with individual organisation's decision maker(s) who in this case are considered agents. The principles or rules previously communicated to the internal decision maker are then disseminated to the organisation's employees. In this step the internal decision maker becomes the principal and the employees the agent. The issue here is the appropriate communication of policies from the top principal (policy make or regulator) to the agents (employees) at the bottom and is known as the 'Principal-Agent problem'. For example, if the policy maker defines principles that it requires organisations to follow, these principles need to be ingrained in any controls the internal decision makers set for their employees.

This is in common with very many other economic activities, such as the mechanism of government and the separation of ownership and management of firms. As Arrow[5] explains, the heart of principal agent problems stems from the misalignment of risk preferences between principals and agents and the cost of monitoring agents by the principal. Agents seek to maximise their revenues, they can do this by taking more risk with the capital provided to them by the principals and creating an incentive problem. This incentive problem can be mitigated by: a) placing rules based restrictions on activities or b) contractually aligning the incentives of the agents to the principals.

It is difficult to place the CNI Principal-Agent problem without the public policy context and vice versa it is inappropriate to define the public policy role of CNI without understanding the atomic nature of the individual Principal-Agent problem within the firm structure.

[5] Essays in Theory of Risk-Bearing by Kenneth Arrow

7.3.2 Diminishing Marginal Returns to Security Investment

A key theme in the above example is the cost of investment in security provision of the ecosystem and monitoring the individual agents in this system. A key tenet of the security economics literature (see Gordon and Loeb[6] for a summary) is that the level of risk is (on average) decreasing in investment and monitoring (in the case of efficient investment and monitoring strictly decreasing) and that the rate of decrease is again diminishing with extra investment. The term monitoring costs includes all costs associated with aligning incentives (that reduce the need for supervision) and opportunity costs created by engaging in this activity.

A simple two dimensional model is as follows, x and y are investments in security technology and monitoring respectively. The principals problem is to minimize the following problem, by changing x and y, min (L(z)S(x,y;z) + x + y). Where S(.) is a risk function that translates investment in technology and monitoring into a residual vulnerability of loss against an amount at risk L from a security breach, given a set of environmental conditions contained in z.

In extensions of this model, L(.) is itself a function of the vector of variables z, which also enters the risk function. For instance this vector may incorporate a feedback from the size of the loss to the probability of a successful attack, or in the case of externalities, z might contain the deviations of other firms requirements for a global welfare maximising level of investment in monitoring and technology (a technological externality). The salient point is that when a firm computes its optimal stance it only includes costs that are directly relevant to it. If these are the sum of all costs in the economic system then a pareto efficient outcome is achievable (social welfare is maximised). However, if some costs to other firms by a particular firm's choices are not internalised by that specific firm, then social welfare cannot be maximised without some form of social coordinator assigning property rights. These property rights then adjust the cost function to account for the externalities (and hence they are internalised).

Consider the risk management case. In an interdependent economy the risk appetite of a firm affects itself and other firms. If the cost of this risk sharing is not distributed across firms in a manner that is appropriately weighted, e.g. assignment of liability claims (the property right), then firms will only cost in their own risk and not that of other firms in the market. When firm weights are highly asymmetric firms are incentivised to dump risks rather than pool them. In a CNI context, using electricity delivery as the example, the electricity distributors and generators may not appropriately secure their own assets connected to electricity transmission systems and assets against cyber threats. This is because they assume that the transmission operator, National Grid, will undertake the cost of protection (having the higher weighting in the economy).

[6] The economics of information security investment by Lawrence Gordon and Martin P. Loeb.

Nesting this problem within a complex ecosystem linked by z, we can create an eclectic family of models that capture many of the observed phenomena documented in the practitioner literature (see Anderson[7]).

Atomised models such as those outlined in the previous sections can be added together using conventional utility functions to monetise losses of different types, including cyber risks being materialised. This form of multi-attribute utility theory is commonly used in security policy to assist in the monetisation and cross addition of losses from various types of security breach, see for instance (Ioannidis, Pym and Williams[8]).

7.4 The Role of Public Policy

Once a model of the threat environment and the interaction of the dimensions of investment, risk and environment has been mapped, the next step is to understand the interaction of policy in the creation (or erosion) of incentives to effectively manage risk.

In security policy scenarios the models have three classes of actors, which have been mentioned in earlier parts of this section, but are presented again for clarity:

- Policy makers or regulators that have objective functions based on broad social welfare targets. In the case of National Grid and the electricity transmission network, the regulator is DECC.
- Agents (usually thought of as representing firms or groups of firms)
- Antagonists, (agents that create risk within the system).

Policy makers enact policy through several mechanisms:

- Passive policy (for instance facilitating information sharing between agents allowing for collective optimal decision making, setting out guidance on appropriate behaviours). A risk based regulatory framework can be an example of a passive policy where principles are communicated to individual organisations decisions makers to adhere to.
- Active policy:
    - Imposing punishments on revealed antagonists such as fines for employees committing gross misconduct in particularly sensitive environments such as CNI.
    - Requiring particular behaviours of the agents that are exposed to risk (with punishments for non-compliance). This is a rules based system where specific requirements are imposed on the agents below.
    - Providing global insurance to agents in the event of loss for a particular level of rent.

Economic theory focuses on efficient distribution of resources to participants in an economic system. Pareto efficiency implies that social welfare is maximised via a

[7] Security engineering: a guide to building dependable distributed systems by Ross Anderson
[8] Information Security Trade-Offs and Optimal Patching Policies by C. Ioannidis, D. Pym and J. Williams.

process where each participant maximises their own utility function over a set of preferences and through continuously optimising individually, there is a gradual convergence towards a maximum social welfare point. The optimisation is assumed to produce a social welfare optimum in the absence of externalities between agents. Externalities refer to direct and indirect effects on other agents not accounted for in by other welfare maximising agent in their own utility functions.

A good set of examples stem from the public goods literature on externalities that are not internalised by individual agents. Tragedy of the commons problems involve public goods for which the sustainability of the public good is often not sufficiently weighted by the group of individuals utilising this good. Grazing rights on public land are a good example of externalities in public goods.

For individual firms within an economic system regulation is formed from a variety of constraints on behaviour (for instance minimum levels of effort and investment in technological and human security) that have punishments for non-compliance. Policy makers can act as enforcing mechanisms for social coordination problems of information sharing.

A fundamental economic concept is that the presence of externalities creates the need for public policy interventions. This intervention can come in several varieties, for instance a restriction on behaviour to ensure a socially optimal outcome (e.g. forcing individuals with penalties to ensure their computers are updated and secure) or by assigning property rights and liability clauses that distribute costs in a manner that reflects the cost of action on others by individual choices.

For information security the wealth of literature has identified three potential coordination mechanisms:

1. Information sharing and coordination on potential risk vectors. Mechanism: Compulsory reporting of information to an information clearing house that then sets out guidance on risk mitigation (current American approach to cyber security). This assumes that all costs can be identified and allocated by appropriate information sharing mechanisms. Transfers to mitigate externalities are then isolated as direct transfers (e.g. private litigation or via memberships of associations with credentials).
2. Behavioural constraints. Mechanism: Enforcing behaviours via a rules based system or a set of risk targets evaluated by sets of metrics designed by the policy maker or regulator. This sets out behavioural constraints (either via principles or rules) that have penalties associated with non-compliance. These penalties need to reflect the costs not born by individual agents (firms or staff) for their own personal actions.
3. Insurance markets. Mechanism: Compulsory purchasing of insurance from either a monopoly insurer or insurance market. The insurance company then sets behavioural requirements contractually. Two types of insurance market are possible:
    - Compulsory insurance markets, all agents (usually at country level) need to purchase insurance, from either a monopoly or competitive market

- Voluntary insurance, again either from either a monopoly or competitive market.

In the US, insurance for critical infrastructure is being considered as an option to secure these systems. The evidence for this can be found the Terrorism Risk Insurance Act (TRIA) of 2002[9] and an appropriate quotation is provided below:

"In addition to its primary role in recovery, insurance can be a powerful tool in inducing critical infrastructure investments that enhance prevention and response".

Appendix 3 discusses the role of insurance and derivative markets in more detail.

The mechanisms are required in cases whereby an externality exists. Their efficacy is then based on the efficiency (from a global social welfare perspective of the cost of mitigation) in internalising externalities.

Internalising externalities, is the concept by which the cost (or benefit) of an externality is incorporated into an agents utility function (either via joint optimisation or constraint) and as such the potential externality is internalised. From the previous discussion the position of a critical infrastructure provider results in two potential effects:

- First they absorb externalities as a cost of security failure is so high that they are willing to bear the costs of other firms and agents. (positive effect for the other agents, negative effect for the critical infrastructure provider).
- Alternatively a negative effect for the other agents, positive effect for the critical infrastructure provider is that the infrastructure provider's security costs are disproportionately distributed to other agents.

More specifically, in the list of potential mechanisms previously discussed, approach 1 maximises social welfare valid if the attack probability s(x*,y*) for optimal choices of x and y is independent of the choices of other agents (employees) in the system. In the presence of externalities, approach 2 is effective in dealing with externalities, but may not be flexible enough when the problem is extended to a dynamic setting with repeated interactions i.e. the risk generating mechanism changes or the technology of defence renders the imposed constraints irrelevant. Approach 3 is less well researched and an example discussion can be found in Appendix 3.

7.5 Remarks

This section has reviewed potential areas of public economics that could be applied to the regulation of various types of firms, individually and in groups. We have reviewed the various types of mechanisms that can allow risks to develop and the methods commonly used in economics to mitigate or monetize them. We have outlined the pros and cons of three mechanisms of risk sharing: public policy based approaches with self

[9] Wharton Risk Management and Decision Processes Center (2005) "TRIA and Beyond: Terrorism Risk Financing in the U.S." The Wharton School, University of Pennsylvania.

insurance, insurance markets (monopoly and competitive) and market based approaches using derivatives contracts.

8. Conclusion

In this report, the first version of National Grid's requirements, we have given a background to National Grid's business and the scope of its input to the SECONOMICS project being the electricity transmission network. Following this we discussed the stakeholders and our engagement plan with them. Having set up our security methodologies and framework in section 5 we described the different security aspects of the current and future states of CNI within National Grid in section 6.

From this we have started the discussion on the different regulatory frameworks (risk and rules based) that could be applied to organisations operating CNI, such as National Grid, as well as different policy mechanisms and their economic justifications.

In the final version of National Grid's requirements we will:

- Look at the security aspects of the current and future states in more detail to determine a high level threat assessment in both states through utilising our key stakeholders
- Understand both the UK and US regulatory frameworks for organisations operating CNI such as National Grid
- Use the NERC-CIP regulatory framework in the US as the most appropriate example of a rules based framework. This, together with the background on policy mechanisms described here, we will assess which regulatory framework will work best for National Grid and other owners and operators of CNI in the current and then future states.

9. 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. Standard CIP-002-4a Cyber Security - Critical Cyber Asset Identification. North American Electric Reliability Corporation (2012).
3. Essays in the Theory of Risk-Bearing. Arrow, Kenneth J. (1971). North-Holland Pub. Co., Amsterdam. ISBN 0-7204-3047-X.
4. Market Signalling: Informational Transfer in Hiring and Related Screening Processes. Spence, A. M. (1974). Cambridge: Harvard University Press.
5. 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
6. Security engineering: a guide to building dependable distributed systems. Anderson, Ross (2008). New York: John Wiley. ISBN 0-470-06852-3. http://www.cl.cam.ac.uk/~rja14/book.html.
7. Information Security Trade-Offs and Optimal Patching Policies, C. Ioannidis, D. Pym and J. Williams, European Journal of Operational Research, Volume 216, Issue 2, 16 January 2012, Pages 434-444
8. Fixed Costs, Investment Rigidities, and Risk Aversion in Information Security: A Utility-theoretic Approach, C. Ioannidis, D. Pym and J. Williams, To appear, Proc. WEIS 2011, Springer-Verlag George Mason University, Fairfax, Virginia, 14-15 June, 2011: WEIS 2011.
9. Wharton Risk Management and Decision Processes Center (2005) "TRIA and Beyond: Terrorism Risk Financing in the U.S." The Wharton School, University of Pennsylvania.

Appendix 1

In this Appendix we present a table of Business Impact Levels (BILs) compiled from a number of BIL tables in HMG IS1[10].

Table 3 - Business Impact Levels 0 to 6 for Sub-Categories of State affairs, International Relations, Economy, Finance, Public services and safety

Sub Category	BIL 0	BIL 1	BIL 2	BIL 3	BIL 4	BIL 5	BIL 6
Impact on life and safety	None	None	Inconvenience or discomfort to an individual	Risk to an individual's personal safety or liberty	Risk to a group of individual's security or liberty	Threaten life directly leading to limited loss of life	Lead directly to widespread loss of life
Impact on political stability	None	None	None	Minor loss of confidence in Government	Major loss of confidence in Government	Threaten directly the internal political stability of the country or friendly countries	Collapse of internal political stability of the country or friendly countries
Impact on foreign relations	None	None	None	Cause embarrassment to Diplomatic relations	Materially damage diplomatic relations (e.g. cause formal protest or other sanctions).	Raise international tension, or seriously damage relations with friendly governments	Directly provoke international conflict, or cause exceptionally grave damage to relations with friendly governments
Impact on provision of emergency services	None	Minor disruption to service activities that requires reprioritisation at the local level to meet expected levels of service	Minor disruption to emergency service activities that requires reprioritisation at the area or divisional level to meet expected levels of service	Disruption to emergency service activities that requires reprioritisation at the county or organisational level to meet expected levels of service	Disruption to emergency service activities that requires reprioritisation at the national level (e.g. one police force requesting help from another) to meet expected	Disruption to emergency service activities that requires emergency powers to be invoked (e.g. military assistance to the emergency services) to meet expected levels of	Threaten directly the internal stability of the country or friendly countries leading to widespread instability

[10] HMG Information Assurance Standard No. 1 – Technical Risk Assessment v3.51

Sub Category	BIL 0	BIL 1	BIL 2	BIL 3	BIL 4	BIL 5	BIL 6
					levels of service	service	
Impact on public finances	None	Loss to Public Sector of up to £10,000	Loss to Public Sector of up to £1 million	Loss to Government/Public Sector of £millions	Loss to Government/ Public Sector of £10s millions, up to £100 million	Short term material damage to national finances or economic interests (to an estimated total of £100s millions to £10 billion)	Major, long term damage to the country's economy (to an estimated total in excess of £10 billion)
Inconvenience and impact on public confidence in public services	None	Likely to reduce an individual citizen's perception of that service (e.g. a compromise leading to the cancellation of a hospital appointment)	Likely to reduce the perception of that service by many citizens (e.g. compromise leading to an outpatient clinic closing for a day, with cancellation of appointments)	Likely to result in undermined confidence in the service provider generally (e.g. public failures at a hospital leading to noticeable lower public confidence in that hospital)	Likely to result in undermined confidence in the service at a national level (e.g. compromise of national patient information databases leading to undermined confidence in national health services)	May lead to a loss of public trust in the service severe enough to cause a noticeable drop in citizens using the service through mistrust, with consequent risk to life	May lead to a complete breakdown in public trust, black market services thrive, consequent widespread loss of life or critical impact on continuity of government
Impact on non-public finances	None	Minor financial loss to an individual or business (typically up to £100)	Significant financial loss to an individual or business	Severe financial loss to any individual such as unemployment or loss of a small business	Devastating financial loss for an individual, or severe economic loss leading to loss of a large company or employer or a number of small businesses	Material financial loss to the country's economy, leading to loss of a number of large organisation or severe damage to entire market sectors	Extensive financial losses across the economy leading to significant long-term damage to the country, such as wide spread unemployment and recession

Sub Category	BIL 0	BIL 1	BIL 2	BIL 3	BIL 4	BIL 5	BIL 6
Locally provisioned services with an impact on the personal safety of citizens (e.g. sheltered accommodation)	None	None	Low risk to an individuals personal safety (e.g. the compromise of the address of a victim of abuse, where there is a low risk of further abuse if such information became known)	Directly lead to a risk to an individuals personal safety (e.g. the compromise of the address of a victim of abuse, where there is a reasonable risk of further abuse if such information became known)	Serious risk to any individual's personal safety (e.g. the compromise of the address of a victim of abuse, where serious further abuse is likely if such information became known)	Threaten life directly (e.g. the compromise of witness protection information, where there is a real risk of attempted murder if the information became known)	Directly threaten or lead to wide spread loss of life (particularly social care and environmental health services)
Locally provisioned services in support of the Civil Contingencies Act	None	Isolated or minor incident to which a Local Authority is not able to react within a few days which affects a small number of citizens	Isolated or minor incident to which a Local Authority is not able to react within a few days which affects a number of citizens/local businesses	Significant incident to which a Local Authority is not able to react within 24 hours which affects a large number of citizens/local businesses - e.g. significant flooding, fire, contamination or explosion.	Major incident to which a Local Authority is not able to react within 24 hours which affects a large number of citizens/local businesses - e.g. major flooding, fire, contamination, explosion or CNI failure.	Major incident to which a Local Authority is not able to react within 12 hours which affects a large number of citizens/local businesses - e.g. major flooding, fire, contamination, explosion or CNI failure	Major incident to which several Local Authorities are not able to react within 12 hours which affects a large number of citizens/local businesses - e.g. major flooding, fire, contamination, explosion or CNI failure.
Utilisation of Public Services	None	Minimal disruption or inconvenience in service delivery to an individual. For example an individual has to re-submit an address or re- register for a service.	Minimal disruption to a group of individuals or significant disruption in service delivery or distress to an individual. For example availability to a set of personal information is lost, requiring	Significant disruption to service delivery for a number of individuals, such as nation wide. For example loss of ability to deliver a non-essential service nation wide	Substantial disruption to service delivery to a large group of individuals, perhaps nationally. Lack of services may directly threaten the safety or wellbeing of an individual or a small group. For example,	Severe disruption to service delivery to a large group of individuals, that may directly threaten safety or lead to limited loss of life, for example limited loss of sensitive police records.	Severe and widespread disruption to service delivery, which may directly lead to widespread loss of life, for example severe loss of availability of many medical records

Sub Category	BIL 0	BIL 1	BIL 2	BIL 3	BIL 4	BIL 5	BIL 6
			resubmission of identity evidence before minor services can be delivered (e.g. library lending)		loss of personal entitlement information for social security payments		
Personal Finance	None	Minor loss of money for an individual, no more than an individual annoyance	Major financial loss for an individual, but not involving any financial hardship, or minor loss for a small group of individuals	Significant loss of income for an individual, such that it has a short-tem impact on the individual's way of life or causes some financial hardship.	Substantial loss of income for a significant group of individuals that causes financial hardship. Financially devastating for an individual for example personal bankruptcy and repossession of home.	Financially devastating for a large group of individuals for example wide spread personal bankruptcy and repossession of homes.	Financial impacts are wide spread to the extent that major long-term damage is caused to the country's economy.

Table 4 - Business Impact Levels 0 to 6 for Sub-Categories of CNI

Sub Category	BIL 0	BIL 1	BIL 2	BIL 3	BIL 4	BIL 5	BIL 6
Communications	None	Local loss of telecoms for a few hours	Local loss of telecoms for up to 12 hours	Local loss of telecoms for up to 24 hours	Loss of telecoms in a region for up to 24 hours	Loss of telecoms nationally for up to a week	Loss of telecoms nationally for more than 1 week
Power	None	Local outages causing disruption for a few hours	Local outage causing disruption for up to 12 hours	Loss of power in a region causing disruption for up to 24 hours	Loss of power in a region causing disruption for up to a week	Loss of power in a region causing disruption for more than 1 week	Loss of power nationally affecting the whole of the country for more than 1 week
Finance	None	Minimal impact (less than £10,000)	Minor loss to a Financial Company (less than £1 million)	Major loss of a Leading Financial company of £millions	Major loss of a Leading Financial Company of £10s millions	Severe losses to the country's business of up to £100s millions	Severe financial losses to the country's business of £10s billions
Transport	None	Minor disruption of a key local transport systems for up to 12 hours	Minor disruption of a key local transport systems for up to 24 hours	Disruption of a number of key local transport systems for up to 24 hours	Major disruption of key regional transport systems for up to a week	Severe national disruption of key transport systems for up to a month	Severe national disruption of key transport systems for over a month
Water and Sewage	None	Breakdown of local water supplies and/or sewage service for a small number (<10) of people for more than a day	Breakdown of local water supplies and/or sewage service for a small number (<50) of people for more than a week	Breakdown of local water supplies and/or sewage service for a number (up to 100) of people or prolonged drought (up to 1 months)	Breakdown of local water suppliers and/or sewage service for over 100 people or prolonged drought (up to 1 months)	Breakdown of regional water suppliers and/or sewage service (effecting >100 people) or prolonged drought (up to 3 months)	Total breakdown of national water supplies and/or sewage service (effecting >100 people) or prolonged drought (> 3 months)
Food and Consumables	None	Local disruption to the distribution of some essential goods, fuel, raw materials, medicines and/or food for up to a week	Local disruption to the distribution of some essential goods, fuel, raw materials, medicines and/or disruption of food for up to a month	Regional disruption to the distribution of some essential goods, fuel, raw materials and medicines and/or widespread disruption of food for up to a week	Regional disruption to the distribution of some essential goods, fuel, raw materials and medicines and widespread disruption of food for up to a month	National disruption to the distribution of essential goods, fuel, raw materials and medicines and widespread disruption of food for up to a month	National disruption to the distribution of essential goods, fuel, raw materials and medicines and widespread disruption of food for over a month

Appendix 2

In this Appendix we present the relevant threat and risk tables from HMG IS1[11] referenced within this document.

Table 5 gives the metrics for Threat Actor Capability which ranges from 1 (Very Little) to 5 (Formidable).

Table 5 - Threat Actor Capability

Motivation	Description
5 – FORMIDABLE	Where the threat actors are resourced by a threat source with Formidable capability, i.e. in addition to lower capabilities can: - Devote a several man-months or even years to penetrating a system - Use specially developed bespoke attacks - Deploy a large amount of equipment - Deploy physical attacks to facilitate further technical compromise Typically a full-time-well-educated computer expert
4 – SIGNIFICANT	Where the threats actors, can - Devote between a few man-months or a few man-weeks to penetrating a system - Adapt publicly available attack tools for specific targets - Deploy a large amount of equipment - Deploy physical attacks to facilitate further technical compromise Typically a full-time well-educated computer expert
3 – LIMITED	Where the threats actors can: - Devote a few man-weeks or days to penetrating a system - Use well-known publicly available attack tools - Deploy a small amount of equipment Typically a trained computer user
2 – LITTLE	Where the threats actors can: - Devote a few man-hours or days to penetrating a system - Deploy a small amount of equipment Typically an average untrained computer user
1 – VERY LITTLE	Where the threats actor has almost no capabilities or resources, i.e. can: - Devote a few hours to penetrating a system using only the equipment already connected to the system - Use simple plug and play devices and removable media

[11] HMG Information Assurance Standard No. 1 – Technical Risk Assessment v3.51

Table 6 gives the metrics for Threat Actor Capability which ranges from 1 (Very Low - Indifferent) to 5 (Very High - Focused). In HMG IS1 there a judgement that the more a potential threat actor is background security checked prior to commencing their role the lower their motivation is to compromise the relevant systems. In Table 6 we make reference to three different levels of background security checks which are:

- Uncleared: No or very little background security check. This can often apply to contractors, visitors etc.
- Basic: Standard commercial organisation background security checks which could include reference, employment, educations and basic criminal checks.
- Extensive: A more in-depth background security check that includes a financial check, employment checks that go back a minimum of 5 years, education checks, detailed criminal background and counter terrorism checks.

Table 6 - Threat Actor Motivation

Motivation	Description
5 – VERY HIGH (FOCUSED)	It is assessed that the threat actor's prime aim is to attack the system. With a very substantial (>~1000) Uncleared threat actor group normally it should be assumed that some will fall into this category
4 – HIGH (COMMITTED) (Maximum for Basic check cleared threat actors) (Maximum for deterrable Uncleared threat actors)	It is assessed, taking any formal clearances into account and whether they could be deterred, that the threat actor will attempt to attack the system on a frequent or constant basis. With a substantial (>~100) Uncleared threat actor group normally it should be assumed that some will fall into this category.
3 – MEDIUM (INTERESTED) (Maximum for Extensive check cleared threat actors) (Maximum for deterrable Basic check cleared threat actors)	It is assessed, taking any formal clearances into account and whether they could be deterred, that the threat actor will attempt to attack the system if the opportunity arises fortuitously or the attack takes minimal effort. With a substantial (>~100) Basic check threat actor group it should be assumed that some will fall into this category.
2 – LOW (CURIOUS) (Maximum for deterrable Extensive check cleared threat actors)	It is assessed, taking any formal clearances into account and whether they could be deterred, that the threat actor may casually investigate or attack the system if exposed to it, but will not seek the system out to attack it. With a substantial (>~100) Extensive checked threat actor group it should be assumed that some will fall into this category.
1 – VERY LOW (INDIFFERENT)	It is assessed, taking any formal clearances into account and whether they could be deterred, that the threat actors will not attack the system.

Table 7 presents a matrix of the product of Capability and Motivation which leads to Threat Level.

Table 7 - Threat Levels as a product of Threat Actor Capability and Motivation

		Capability Level				
		1 VERY LITTLE	2 LITTLE	3 LIMITED	4 SIGNIFICANT	5 FORMIDABLE
MOTIVATION	1 INDIFFERENT	Negligible	Negligible	Low	Low	Moderate
	2 CURIOUS	Negligible	Negligible	Low	Moderate	Substantial
	3 INTERESTED	Negligible	Low	Moderate	Substantial	Severe
	4 COMMITTED	Low	Low	Moderate	Severe	Severe
	5 FOCUSED	Low	Moderate	Substantial	Severe	Critical

Table 8 presents a matrix of the product of Business Impact Levels and Threat Levels which gives the Risk Level.

Table 8 - Risk Levels as a product of Business Impact and Threat Level

		Threat Level					
		Negligible	Low	Moderate	Substantial	Severe	Critical
Business Impact of Risk Realisation (Business Impact Level - BIL)	BIL0	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low
	BIL1	Very Low	Very Low	Very Low	Low	Low	Low
	BIL2	Very Low	Low	Low	Medium	Medium	Medium
	BIL3	Very Low	Low	Medium	Medium	Medium-High	Medium-High
	BIL4	Low	Medium	Medium	Medium-High	High	High
	BIL5	Medium	Medium	Medium-High	High	High	Very High
	BIL6	Medium	Medium	Medium-High	High	Very High	Very High

Appendix 3

In this appendix we provide further technical information on the economics of setting public policy and associated problems that are discussed in Section 7. Specifically, more information is provided on the following topics:

- Principal-Agent problem in risk management
- Insurance as a social co-ordinator
- The role of a market based solution.

Principal-Agent problem in risk management

Modern information ecosystems generally have multiple interactions with information passed between agents through many layers. When a principal asks an agent to handle, store and process data, the agent is, in general, not the sole actor working on behalf of the principal. At any given point there is a sequence of principals and agents passing information between them and sharing and seeking rents for each part of the service. Complete alignment of incentives in this situation is unlikely.

Take for instance a simple example system, the principal prices a service that he needs provided for a particular economic activity. Assuming that through economies of scale, flexibility and scalability he has a sequence of agents performing these tasks. The service requires both rent from the principal and information, which is then processed and returned to the principal.

The first agent receives the rent and information from the principal and contracts to undertake the service. This agent acts as a coordinator for a set of atomised services and then distributes payment to this set of secondary agents. Information is similarly broken up between the sub services and the agent coordinates information requirements. Each agent can choose to provide their service using either a high risk (low cost) or low risk (high cost) approach.

Payoffs for agents are proportional to their risk choices. The principal chooses levels of risk and cost for which they are indifferent and this sets the service rent they are willing to pay. A point on this risk-cost set is provided by the series of rewards and punishments that the principal can enact.

However, this efficient provision is based on the assumption that there is no information asymmetry between the various agents and the principal and that the principal can punish (and is incentivised to punish) those undertaking activities that create risk to the principal.

In the case of full information such all risk is priced into the sequence of tasks undertaken by the agents in the system. As such a Pareto efficient outcome is possible. However, it is unlikely that the agents are a) willing or b) able to provide accurate information on the use of the principal's information or fragments of information. Once we assume asymmetric information and/or costly monitoring of agents then an incentive incompatibility can arise. The risk-cost trade-off for the principal achieves an optimum based on a particular set of risk preferences. In the classical economic theory of

contracting (see for instance Spence[12]), risk aversion is a single parameter that defines the welfare effect of changing the relative levels of risk and cost.

If the agents acting on behalf of the principal have lower intolerances to risk and monitoring is extremely costly or impossible then information asymmetry will restrict the principal's knowledge of the agent's behaviour.

At this stage agents will need to choose the level of risk, usually in the form of a level of investment in security and as such they will choose a different point on the risk-cost frontier, a point that achieves a higher level of risk for a lower level of cost, maximising service rent. If principals are unable to compare the distribution of outcomes from the outsourced services to their natively sourced service then an agency problem will begin to manifest itself.

A question that arises: why would principals be unable to construct an informative prior to compare to the service provided by a private organisation? A first answer to this issue is in the elucidation of the risk-cost frontier. Internally sourced services may (and probably will) not be on the frontier proffered by the top level agent. Second, the elements of the risk vector may (and probably will) not be fully measurable. Principals are unlikely to be able to fully understand the nature of the risks of task undertaken prior to the conclusion of its provision of labour. This follows to the third reason, the outcome space and attached probabilities, only with repeated interactions will the principal be able to gauge and apply quantifiable metrics to the risk vector, even if it is fully rationalised.

This information asymmetry then allows agents to decide, in a cloak of relative obscurity, the cost-risk balance to maximise their rents from service coordination and provision. The more layers of interaction the greater the accumulation of risk within the system.

Insurance as a social co-ordinator

One alternative mechanism for the design of regulation for security of firms in complex economic systems is the presence of compulsory insurance. Instead of designing legal frameworks that will require constant updating, insurance companies provide cover for security risks and this provision is rolled over at regular intervals. Part of the coverage requirement is the successful implementation of specific behavioural and technological standard for each firm. Business contracts enforce these standards are firms are given punishments by the social coordinator for not being compliant with their coverage.

The major question in this approach is will insurance companies demand the correct behavioural levels for firms and be able to identify the correct cost for insuring security breaches.

Issues that affect the identification of the correct premium:

Moral hazard: parties that are insured take more risk as the cost of this risk has now been born by the insurer. Without monitoring (see principal agent issue) the insurer

[12] Market Signalling: Informational Transfer in Hiring and Related Screening Processes by A. Spence.

cannot determine the correct premium to charge as the risk of a breach without insurance is less than the risk with insurance.

Adverse selection: with heterogeneous firms and risk types insurance companies need to charge differing premia to appropriately and efficiently allocate protection. When adverse selection is an issue, insurance companies are unable to identify the type of individual or firm that they are insuring. This has two contrasting issues:

- In the case of voluntary insurance:
    - If the individual firm does not know its type then this is less of an issue as an average premium provides actuarially fair insurance for most common risk types.
    - However, in the event that individual firms are able to distinguish their own risk type (e.g. high versus low) the low risk firms will be priced out of the market leaving only high risk firms that buy insurance.
- In the case (suggested above) of compulsory insurance, low risk firms subsidise the high risk firms leading to distortions in their operational function.

For security insurance a pertinent issue is the role of the risk vector. In conventional insurance models the function S(x,y), the risk vector is independent of a) the presence of insurance for a given level of x and y and b) the actions of other agents (representing firms) in the economic system.

For security problems the number and nature of antagonists creating exploits that lead to non-zero levels of residual risk, will be responsive to various elements within the economic system. It would be expected that the presence of insurance and the global choices for insurance would be one input into an attack function.

One postulate for this type of problem would be as follows, S(x,y;z,n(x,y,z)), represents a residual risk function, whereby x and y are choices of the agent, z are externalities from the structure of the economic system and n is a vector of choices as a function of the choices of the firm and the vector z of environmental variables (which could include the presence of insurance as a signal).

From the viewpoint of the insurer, if the number of firms to be insured is very large then profit can be viewed as a product of total value of insurance premiums charged – (total expected payouts – deductibles). For actuarially fair insurance in the presence of a monopoly insurer this should be equal to the global level of risk aversion of the agents in the system (the amount of compensation individual agents pay to return to a certainty equivalent in the amount of a loss). This value is a function of total risk.

As such insurance companies extract the surplus from the economic agents in the system that arises from the natural level of risk aversion. At present there is a debate in the economic literature on whether firms can be modelled as being risk averse in information security, see Ioannidis, Pym and Williams[13] for an overview. In the case of critical infrastructure one aspect of policy is the imposition of risk aversion on a firm, from its stakeholders.

[13] Fixed Costs, Investment Rigidities, and Risk Aversion in Information Security: A Utility-theoretic Approach by C. Ioannidis, D. Pym and J. Williams

The presence of competitive or contestable insurance markets changes the role of insurance in a social coordination context. First, dividing the market between insurers (or in the case of a contestable market replacing a monopoly insurer with another if they extract more than the actuarially fair surplus) results in the complete elimination of any potential coordination effect (each insurer is only interested in their slice of the market, or the level of risk needs to be higher to extract a higher actuarially fair premium).

The problem of insurance increases, if insurance companies have differentiable policy types and an inability to identify the level of risk of those being insured choosing their contracts. As such an initial conclusion is that compulsory insurance will not act as a coordinator to mitigate externalities.

The role of a market based solution

An extension of insurance based models for mitigating the costs of security breaches arises from the use of marketed contracts with payoffs that are negatively correlated with the costs of attacks. A simple mechanism for actively managing the cost of security risk is for a properly functioning security risk derivatives contract (security in this case not to be confused with an investment contract).

Example: A security futures contract, based on a security index. Consider the j firm from a set of N firms in an economic system. For a vector of k from K attributes a count of *realised* losses $v_{i,j,k}$ for a given month or quarter indexed by i is recorded using a standardized auditing procedure. An example could be the dollar amount of losses incurred by a loss of data or damages to a physical piece of infrastructure from a cyber attack.

A weighted index for the level of attacks would be of the following form,

$$I_i = \sum_{k=1}^{K} \sum_{j=1}^{N} \omega_k w_j v_{i,j,k}$$

where w_j is the turnover weighting of the j firm and ω_k is the weighting of the k loss component in the index. A futures contract $F(t,T)$ would be a delivery price of a contract equivalent to a fixed amount H times the index value at I_T. For a given company purchasing $\beta_j = \mathrm{cov}\left(v_{i,j}, I_i\right)\mathrm{var}^{-1}\left(I_i\right)$ futures contracts times the total turnover w_j would create a partial hedge against security risk over the time period t,T.

The variance of the index $\mathrm{var}\left(I_i\right)$ and the covariance with a particular firms $\mathrm{cov}\left(v_{i,j}, I_i\right)$security risk profile would be properties that are emergent from the risk structure previously described in the insurance section. The advantages of such a contract would be as follows:

1. A liquid contract would allow a firm to dynamically rebalance security protection.
2. The level of security risk could be tailored from a complete hedge to a partial hedge of security risk.

3. A liquid futures market should (under standard models of informational efficiency) price future cyber threats quickly.
4. Multiple time horizons could negate the issue of differing discount rates between social planners and firms in repeated security games (a term structure of security risk).

Issue for derivative contracts in this setting:

1. The evolution of the index benchmarking, the security prices must be a semi-martingale (i.e. no single agent could effect the price of the index prior to delivery of the futures contract in a deterministic manner, therefore gaining a no-free-lunch-with-vanishing-risk trading strategy).
    a. This issue is very hard to negate and has been a problem for futures contracts priced on artificial indices in the past (see LIBOR scandal 2012).
    b. A sophisticated attacker could use futures contracts to realise money from attacks without having to actually steal value from individual firms. The attacker would simply need to destroy value across a large number of firms whilst being long in the futures contract.
2. Systemic security risk will not be captured by such a contract, see second point from above, for an example of this.
3. There is no mechanism to compel improved security behaviour amongst agents in the economic system.
4. There are deadweight costs for leveraging security risk that may be unforeseen at the inception of the contract (e.g. moral hazard problems, speculative bubbles).

For a futures market to exist a regulator would need to set and enforce rules on the mechanism that creates the risk via the antagonists generating losses for the firms in the index.

Appendix 4

Standard CIP-002-4a Cyber Security - Critical Cyber Asset Identification by NERC has been included in the Appendix as a separate annex.

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-3a

3. Purpose: NERC Standards CIP-002-3 through CIP-009-3 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-3 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

4. Applicability:

4.1. Within the text of Standard CIP-002-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-002-3:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

B. Requirements

R1. Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.

R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.

R1.2. The risk-based assessment shall consider the following assets:

R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.

R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System.

R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.

R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.

R1.2.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.

R1.2.7. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

R2. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-3, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

R4. Annual Approval — The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of

the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

M1. The Responsible Entity shall make available its current risk-based assessment methodology documentation as specified in Requirement R1.

M2. The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R2.

M3. The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R3.

M4. The Responsible Entity shall make available its approval records of annual approvals as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-002-3 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	January 16, 2006	R3.2 — Change "Control Center" to "control center"	Errata
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3	
3	December 16, 2009	Approved by the NERC Board of Trustees	Update
3a	May 9, 2012	Adopted by the NERC Board of Trustees	

Appendix 1

Requirement Number and Text of Requirement
R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics: R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, R3.2. The Cyber Asset uses a routable protocol within a control center; or, R3.3. The Cyber Asset is dial-up accessible.
Question 1
Is the phrase “Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange” meant to be prescriptive, i.e., that any and all systems and facilities utilized in monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange, must be classified as Critical Cyber Assets, or is this phrase simply meant to provide examples of the types of systems that should be assessed for inclusion in the list of Critical Cyber Assets using an entity’s critical cyber asset methodology?
Response to Question 1
The phrase “Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange” is illustrative, not prescriptive. It simply provides examples of the types of Cyber Assets that should be considered. It does not imply that the items listed must be classified as Critical Cyber Assets, nor is it intended to be an exhaustive list of Critical Cyber Asset types.
Question 2
What does the phrase, "essential to the operation of the Critical Asset" mean? If an entity has an asset that "may" be used to operate a Critical Asset, but is not "required" for operation of that Critical Asset, is the asset considered "essential to the operation of the Critical Asset"? Remote access to the systems is valuable to operations (see Material Impact Statement below), but operation of the Critical Asset is not literally dependent on these laptops.
Response to Question 2
The word “essential” is not defined in the *Glossary of Terms used in NERC Reliability Standards*, but the

well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "essential to the operation of the Critical Asset" means inherent to or necessary for the operation of the Critical Asset.

A Cyber Asset that "may" be used, but is not "required" (i.e., a Critical Asset cannot function as intended without the Cyber Asset), for the operation of a Critical Asset is not "essential to the operation of the Critical Asset" for purposes of Requirement R3. Similarly, a Cyber Asset that is merely "valuable to" the operation of a Critical Asset, but is not necessary for or inherent to the operation of that Critical Asset, is not "essential to the operation" of the Critical Asset.