SECONOMICS

D2.3 – National Grid Requirements, Final version

R. Coles (NGRID), R. Ruprai (NGRID), M. Collinson (UNIABDN), D. Pym (UNIABDN), J. Williams (UNIABDN)

Document Number	D2.3
Document Title	National Grid Requirements Final Version
Version	1.0
Status	Final
Work Package	WP 2
Deliverable Type	Report
Contractual Date of Delivery	31.01.2013
Actual Date of Delivery	31.01.2013
Responsible Unit	NGRID
Contributors	UNIABDN, UNITN, Fraunhofer
Keyword List	CNI
Dissemination level	PU

SECONOMICS Consortium

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

1	UNIVERSITÀ DEGLI STUDI DI TRENTO	Università Degli Studi di Trento (UNITN) 38100 Trento, Italy www.unitn.it	Project Manager: prof. Fabio MASSACCI Fabio.Massacci@unitn.it
2	DEEPBLUE	DEEP BLUE Srl (DBL) 00193 Roma, Italy www.dblue.it	Contact: Alessandra TEDESSCHI Alessandra.tedeschi@dblue.it
3	Fraunhofer ISST	Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., Hansastr. 27c, 80686 Munich, Germany http://www.fraunhofer.de/	Contact: Prof. Jan Jürjens jan.juerjens@isst.fraunhofer.de
4	Universidad Rey Juan Carlos	UNIVERSIDAD REY JUAN CARLOS, Calle TulipanS/N, 28933, Mostoles (Madrid), Spain	Contact: Prof. David Rios Insua david.rios@urjc.es
5	UNIVERSITY OF ABERDEEN	THE UNIVERSITY COURT OF THE UNIVERSITY OF ABERDEEN, a Scottish charity (No. SC013683) whose principal administrative office is at King's College Regent Walk, AB24 3FX, Aberdeen, United Kingdom http://www.abdn.ac.uk/	Contact: 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	07/12/2012	Draft	R.Coles (NGRID), R.Ruprai (NGRID), M. Collinson (UNIABDN), D. Pym (UNIABDN), J.Williams (UNIABDN)	Initial Draft
0.11	14/12/2012	Draft	E. Chiarani (UNITN)	First quality check completed of earlier skeleton draft: minor remarks and changes
0.2	14/12/2012	Draft	R.Coles (NGRID), R.Ruprai (NGRID), M. Collinson (UNIABDN), D. Pym (UNIABDN), J.Williams (UNIABDN)	Second Draft following multiple internal NGRID & UNIABDN reviews
0.3	21/12/2012	Draft	R.Coles (NGRID), R.Ruprai (NGRID), M. Collinson (UNIABDN), D. Pym (UNIABDN), J.Williams (UNIABDN)	Third draft version following comments by NGRID CISO
0.4	18/01/2013	Draft	A. Schmitz (Fraunhofer)	Fourth draft version following scientific review
0.5	25/01/2013	Draft	S. Lane (NGRID)	Fifth draft version following final internal quality review
0.6	29/01/2013	Draft	W. Shim, E. Chiarani (UNITN)	Review of draft by UNITN and some minor changes
1.0	01/02/2013	Final	R. Ruprai (NGRID)	Final version after R. Coles (NGRID) signoff

INDEX

Executive summary

This report presents the final version of National Grid's requirements for Electricity Transmission with respect to Work Package 2 of the SECONOMICS project. It follows on from the work documented in SECONOMICS Deliverable 2.2 titled 'National Grid Requirements – First Version'.

This report presents the requirements for Work Package 2 which focus on understanding and assessing the information/cyber security regulatory frameworks that are or could apply to Critical National Infrastructure operators. National Grid's electricity transmission network in the UK serves as the example that is used to assess these regulatory structures in this work package.

The information/cyber security scenarios of Work Package 2 have been constructed to cover the entire picture of National Grid's UK Critical National Infrastructure in the current state and the short to medium term future. For the current state, both threat and risk assessments are completed for the different business areas in scope. The future state consists of the future and emerging threats that were identified in numerous internal National Grid workshops and external security roundtable meetings.

For regulators, mitigating the risks identified in the current state and potential risks in the future state is achieved through the regulatory structures in place. National Grid, being a regulated entity, has significant experience of the regulatory structures that it is subject to and these are presented in this report.

The security scenarios and discussion on regulatory structures provide a thorough background to progress the building of models, and producing policy recommendations, that will be relevant to Critical National Infrastructure. The aim of this work will look at the following areas:

- To assess whether the current Critical National Infrastructure regulations 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, analyse whether the current regulatory frameworks are flexible and adaptable enough to manage these changes.
- Which regulatory structures would be better in the current and future states? And can we look at examples elsewhere in the world or in other industries?

These areas form the key requirements of this work package.

1. Introduction

This report is the final version of National Grid's Requirements. It builds upon the work undertaken in the earlier report Deliverable 2.2 (D2.2) titled 'National Grid Requirements – First Version'.

The elements of work package 2 are designed to cover the broad area of critical national infrastructure protection through the example of electricity transmission in the UK, which National Grid owns and operates. National Grid (NGRID) is the project partner leading this work package with significant subject matter expertise and experience in information/cyber security aims, concerns, issues and challenges within 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 assessment 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 D2.3 (D2.3) of WP2. Within the wider context of this work package, this document builds upon Deliverable D2.2 (D2.2) and is the final version of the CNI requirements which includes more in-depth requirements assessment and analysis that were not presented in D2.2.

The first report, D2.2, introduced the CNI case study and National Grid's role and responsibilities as a provider, operator and owner of CNI. This report significantly builds upon D2.2 as well as focuses more on the security scenarios and regulations in practice. The more theoretical aspects of regulation and public policy will be considered in work package 6, initially in Deliverable 6.1.

The scope of this report will focus on the security scenarios in the CNI space and the current regulatory structures that National Grid is subject to both in the UK and US. A key objective of the work package will be the potential strategic directions for regulation and cost benefit analyses of implementing different levels/types security.

1.2 Overview of the document

Deliverable 2.2 set the scene and context in a number of areas which are covered in more detail in this document, the final version of the 'National Grid Requirements'. This document is organised as follows:

- Section 2 builds upon Section 3 of D2.2 by providing a further background of the electricity transmission network that National Grid operates as well as details of previous blackout incidents and Supervisory Control And Data Acquisition (SCADA) system malware attacks. This will provide context for the proceeding sections as well as the other WP2 deliverables.
- Section 3 can be seen as a follow on to the stakeholder map presented in Section 4 of D2.2. The stakeholder map presented National Grid's stakeholders at an internal, national and supranational level but it was not clear, at that stage, how we would engage with these different stakeholders. In Section 3 we present an engagement plan showing which groups and forums that National Grid has representation on, which will help us engage with our key stakeholders to facilitate the aims and expected outcomes of WP2 and the wider project.
- Section 4 then moves forward into the 'Current' and 'Future' security scenarios relevant to National Grid as an owner and operator of CNI. This section significantly expands upon Section 6 of D2.2 and goes into the detail of the security impacts, threats and risks using the methodology described in Section 5 of D2.2.
- Section 5 adds to D2.2's introduction to the two methods for the development of regulatory structures within this area: a rules approach versus a principles approach to regulation. In addition, this section provides considerable detail about the two regulatory structures that National Grid is subject to in the UK and US which link to the two main methods of regulation.

1.3 Validation

To validate the contents of this report we have consulted with numerous parties, bilaterally or as part of a larger group, to verify our understanding of the various areas of the report. At a high level these areas are:

- Background and high level technical architecture of the electricity transmission systems
- Previous electricity blackout incidents
- Previous malware incidents affecting SCADA systems
- Security impacts, threat levels and risk assessment of the Current State of National Grid's electricity transmission network
- Security impacts and threat levels of the Future State of National Grid's electricity transmission network
- UK CNI regulatory structure
- US CNI regulatory structure.

A list of the validation activities for both the first (D2.2) and final (D2.3) versions of National Grid's Requirements is given in Appendix 3.

2. CNI Case Study Further Background

In Deliverable D2.2, National Grid Requirements – First Version, we gave a background to the electricity transmission network that National Grid owns and operates in the UK. The process for balancing the network through the observation of the frequency of the system was also described.

In this further background section we describe, in more detail, how the SCADA network is used to manage and balance the electricity transmission network and the numerous sites it is connected to. This information will be essential to understanding the impact of compromise and the motivation for a threat source to attack it, which will be discussed the Section 4.

Please note that we often refer to the electricity transmission network as the 'grid'.

2.1 SCADA Network

In order for the electricity control room systems and the operators to communicate with substations, generators and interconnectors a physical network of fibre optic cables connects them to the control rooms. This physical network can be used to exchange electronic information between them via technologies and protocols such as Internet Protocol (IP), Multiprotocol Label Switching (MPLS), telephony and facsimile.

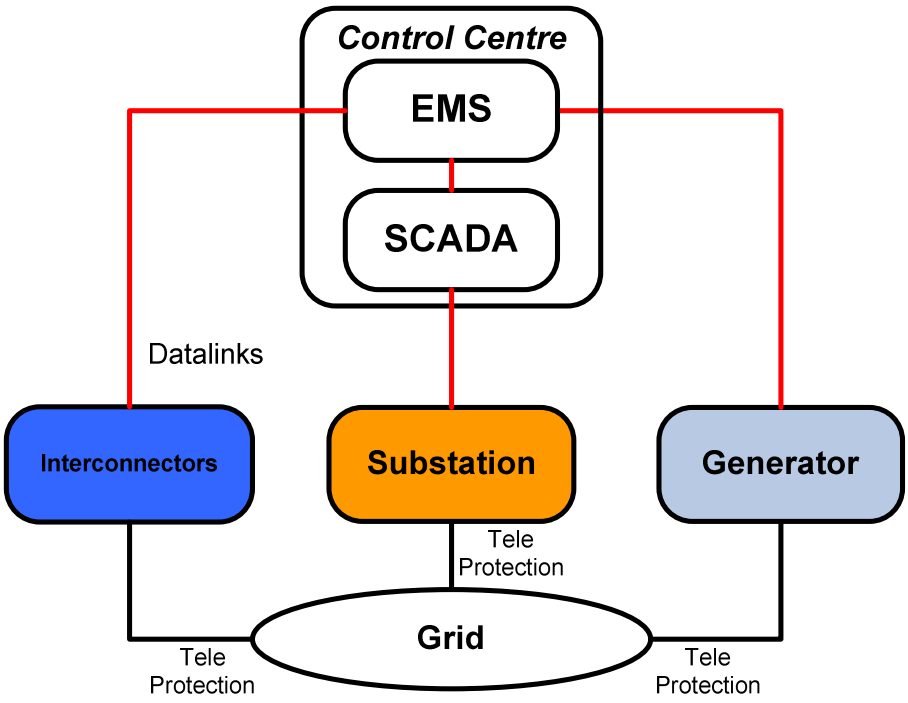

Figure 1 – Data links between the Control Centres, Interconnectors, Generators and Substations

Figure 1 shows the data links between the control centres and the interconnectors, generators and substations. The black lines between the interconnectors, generators and substations denote the actual power lines that connect these entities. Tele-protection systems are in place for safety across the high voltage power lines to stop live wires

coming into to contact with commercial buildings, homes, vehicles and people. This will be discussed further in Security Scenarios section.

The red lines denote the fibre-optic data links that connect the entities to the control centre, specifically the Electricity Management System (EMS), through a front-end processing unit and a SCADA system interacts with the electricity transmission substations. In addition, there are interconnectors, distributers and generators linked to the balancing mechanism which determine demand forecasts and the electricity reserve. This is also discussed in the Security Scenarios section.

Broadly, the information exchanges required from the interconnectors, distribution networks and generators is to balance the electricity across the grid, whilst the SCADA system monitors and manages the grid infrastructure. We will look at these two areas separately to identify the key data needs in order that the electricity transmission network is operating satisfactorily. However, it is important to note that the information is not just travelling in one direction to the control centres. The data links can also be used to send data/information requests as well as commands to the various interconnectors, generators and substations. This is discussed further in the Security Scenarios section.

2.2 Managing the Electrical Transmission Network

A country's electricity transmission grid is essential for the well being of its citizens, economy and government, therefore resilience and availability are necessary and key requirements. Throughout its history, including before the need of cyber security, National Grid has strived to ensure resilience and availability of the UK's electricity transmission network. As a result, for each and every end user of electricity there are a number of transmission lines that can be used to service them. This allows for lines and pylons (towers) to be maintained, replaced and/or relocated without any interruption in the supply of electricity.

Managing the grid involves knowing which transmission lines are operational, their maximum load capacity, when they are due for maintenance work and if they are in immediate need of maintenance work. With this information, the control centres can determine which transmissions lines to take out of action for the relevant maintenance and where and how much electricity load can be spread across the rest of the network.

Without this information there could be a number of both immediate and short-term impacts which are discussed in the Security Scenarios section.

2.3 Frequency Balancing on the Electrical Transmission Network

Due to the fundamental nature of electricity and the constraint that it cannot be stored, the demand and supply on the network must be continually balanced. As explained in Deliverable D2.2, balancing requires the frequency of the network to be kept within a certain tolerance of 50Hz.

Thus, the frequency of the network is monitored continuously. As demand increases, this increases the load on the generators and the frequency drops. To counteract this, generations sites need to be either ramped up or turned on.

For the control centre to be able to quickly respond to demand or supply changes, both expected and unexpected, they need to know the following at the very minimum:

- Current frequency across numerous points in the network
- Current supply at the generation sites including interconnectors
- Spare capacity at the generations sites and interconnectors
- Time required to ramp the generators up and down
- Current demand at the various high voltage substations.

All this information is obtained by the control centres across the SCADA network.

National Grid has many years of experience operating, maintaining and balancing the electricity transmission network. There are many teams that work on forecasting demand in the immediate, short (hours to days), medium (days to weeks) and long (months to years) term. From this forecasting, the control centres determine how much spare capacity is required at all times and this is often referred to as 'reserve'. Without this reserve effective balancing would not be achievable.

2.4 Previous Blackout 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. Whilst the causes of many of these incidents have often been the result of accidents, assessing the impact will provide valuable input to assessing the business impact of cyber security incidents in the Security Scenarios section.

A sample of these incidents has been described below:

- In September 2003 there was a major blackout in Italy cutting service to a total of 56 million people. Italy was mainly affected as well as parts of Switzerland, Austria, Slovenia and Croatia. The blackout was the result of a power line between Switzerland and Italy being damaged causing a cascade effect resulting in generation sites to trip. Consequences of the outage were failures in the public transport sector, the publishing of newspapers and mobile phone links. The health sector continued operating using reserve power generators and the overall initial impact was less dramatic as it happened on a weekend night.
- On 14 August 2003 there was a major blackout in the USA and Canada affecting over 45 million Americans and 10 million Canadians. It was caused by a high-voltage power line which brushed against some overgrown trees in Northern Ohio that resulted in a shut down causing other generation sites to follow. The system which would normally have tripped an alarm in the control room failed. The heat of August triggered the outage, because the energy demand increased as many people turned on fans and air conditioning. The result was a wide-area power failure in the North-eastern USA and central Canada. The affects on the general public was a loss of power for up to two days. Some cities water systems lost pressure, the telephone circuits were overloaded, the cellular service was interrupted, but most television and radio stations remained on the air, because of the help of backup generators. Most of the public transport system and financial markets were interrupted and affected.

- On the 30 July 2012 there was a significant electricity outage in the North of India, which is one of the biggest power failures in the world to date. It was caused by record power demand due to extreme heat. In the Punjab and Haryana states, the agricultural industry used power from the grid for running irrigation pumps as the monsoon session had arrived late. Due to the increased power use, the 400 kV Bina-Gwalior line tripped, which led to the tripping of power stations. The outage affected seven north Indian states and more than 300 million people were without power. Traffic signals were non-operational, some airports and railways were shut down, and this resulted in major transport problems during the Monday morning rush hour. Additionally the health sector was affected as several hospitals, without backup generators, had their health services interrupted. Water treatment plants were also shut down for several hours, leaving millions without water and businesses were impacted due to leaving many unable to operate. After 15 hours 80% of service was restored. However, the following day, the previous affected regions were again without electricity and at the same time the eastern Indian grid failed as well, with the North-Eastern grid tripping out shortly afterwards. The factors leading to the outages were the weak inter-regional corridors due to the multiple outages the day before, the high loading on the Bina-Gwalior-Agra link and the tripping of this link as a result. Most of the 48,000MW demand load was affected but a few regions of the country continued to have power. Half of India was left without an electricity supply and over 620 million people were affected. The electricity was restored in the affected regions between 31 July and 1 August 2012 but the impact on the society was significant, as some hundred thousand people were stuck in the public transport system, airports were using generator backups and 200 miners were trapped underground.

2.5 Previous Malware Incidents affecting SCADA systems and Electricity Transmission Networks

In the previous subsection we discussed a number of significant blackout incidents which have occurred globally in the past. The purpose of this is to understand the cause of the incidents as well as the impact on that country's citizens. In none of these cases were the causes due to a cyber security incident. However, the probability of such attacks is nontrivial and they have the potential to cause similar, if not greater, impacts to those described in the previous subsection.

In recent years there have been information/cyber security incidents on SCADA systems, electricity transmission networks and their operators who are referred to as Transmission Service Operators (TSOs). These all have relevance to National Grid and the CNI it owns and operates. It also provides a basis for the current and future state threat and risk analysis that are presented in Section 4.

Many of the information/cyber security incidents on SCADA systems and Electricity Transmission Networks were caused by malware infecting systems which resulted in the malfunctioning or breaking down of core equipment. Malware software is often created to disrupt computer operations, gather information or to gain access to computer systems.

A sample of these incidents has been described below:

- Between June 2009 and the beginning of 2011 there was a major malware attack on Iran's uranium enrichment program. Before the malware, named Stuxnet, could be finalised and attack the program there had been a prior stage. A cyber espionage tool was used as a precursor to Stuxnet in order to gain information about technical configurations and operations in the plant in Natanz to design the Stuxnet code. Stuxnet was designed to attack the centrifuges used to enrich uranium and, to ensure the attack was not mitigated, also attacked the SCADA systems which provided operational control for the infrastructure and production networks. Its specific purpose was to corrupt the Siemens' Simatic Wincc SCADA system. Stuxnet intercepted commands sent from the SCADA system to control a certain function at the plant. The malware replaced the intercepted commands with malicious commands in order to manipulate the system. This resulted in the malfunction of the SCADA system without anyone recognising the impact on the uranium enrichment. After some changes on the system by the attackers, the worm spread wider than intended. Stuxnet-like malware are highly dangerous, because they are capable not only of affecting computer systems across a network, but they are also able to cause physical damage to the equipment that these computer systems control.
- In 2010, a year after Stuxnet was discovered, another piece of malware using some of the same techniques was found. This malware, named Duqu, infected systems in Europe and it has been presumed that it was written by the same authors behind Stuxnet. Like Stuxnet, Duqu masks itself as legitimate code as a driver file with a valid digital certificate. The difference is that this malware is not a worm as it does not self-replicate in order to spread. It is thought to have been a precursor to a Stuxnet-like attack. Its purpose was to conduct reconnaissance on an unknown industrial control system and gather intelligence for a possible targeted attack later. Whilst not having the components to attack SCADA systems directly, it is still a danger for SCADA systems due to its similarities to Stuxnet.
- In May 2010 the malware Flame, also known as sKyWIper, was created as a cyber espionage tool. Compared to Duqu it is significantly more complex. Flame is an attack toolkit and has worm-like features. These features allow Flame to replicate in a local network and on removable media. Once Flame has infected a system, it begins a complex set of operations, including sniffing the network traffic, taking screenshots, recording audio conversations, intercepting and recording keystrokes on keyboards and so on. The data is then available to the operators and the operators can even expand the functionality after the malware has been deployed. The purposes of the malware are still being investigated, because it contains about 20 modules in total.
- More recently, in November 2012 the German 50 Hertz grid company was the subject of a botnet attack from Eastern Europe. 50 Hertz's web servers were blocked after the attack by the hackers using a Distributed Denial-of-Service-Attack (DDOS). It is believed that the attackers did not aim to disturb the control of the power grid as the computers related to the grid control do not have internet access. The attack resulted in the blockage of their intranet and internet as well as the failure of the e-mail communication internally and externally. The

50 Hertz administrators reacted by disconnecting the computers from the network and closing their website temporarily.

3. 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 owns and operates electricity transmission in the north-eastern region of the US as well as the UK, we will engage with internal, IT-centric 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.

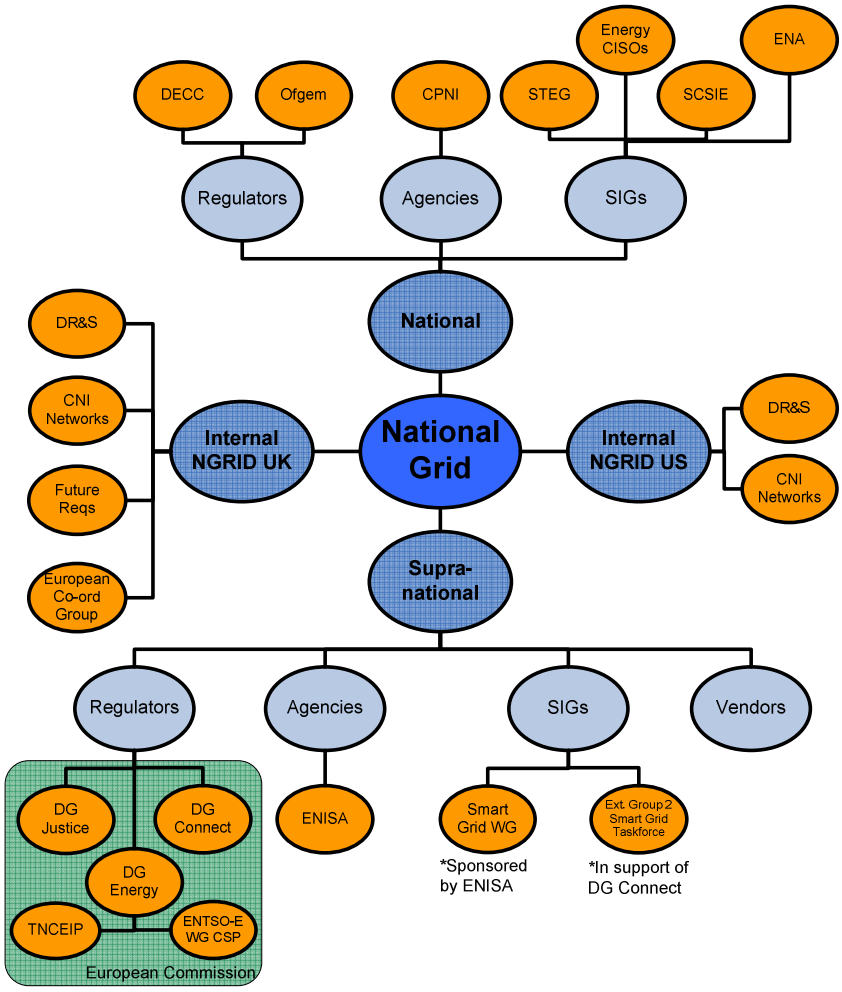

Figure 2- National Grid Stakeholder Map

Acronym	Full name
DR&S	Digital Risk & Security (a department within National Grid)
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
SCSIE	SCADA and Control Systems Information Exchange (Run by CPNI)
ENA	Energy Networks Association
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 3- National Grid Stakeholder acronyms and full names

Figure 2 presents National Grid's stakeholder map for the SECONOMICS project, as presented in D2.2 with a number of additions, and Figure 3 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.

In Deliverable D2.2 we described the aims of our engagement with the stakeholders. However, it was not clear which forums, groups, meeting or workshops would be used to facilitate the engagement with the different stakeholders and stakeholder groups (i.e. Regulators, Government Agencies, Industry and NG internal groups).

It is difficult for a commercial organisation to have regular bilateral engagements with each of the stakeholders and often this will not be as productive as a larger meeting or workshop with fellow industry members. In fact, such bilateral meetings can be counter productive as National Grid would not be airing its expert opinions and views in larger forums and thus not gaining the buy in of the relevant government departments and industry.

Table 1 presents the different national and supranational groups and forums that we are actively engaging with around information security. For each group or forum we detail the frequency of meetings, whether regulators, governmental agencies and/or industry are engaged with via this group and other details about our engagement and attendance of each group.

Table 1 – Engagement with Regulators, Governmental Agencies & Industry

Groups	Regulators	Gov. Agencies	Industry	Freq.	Forum of meetings / workshops & details
ENTSO-E CSP	DG-Energy		EU TSO industry	Quarterly	ENTSO-E is the group of the electricity transmission service operators (TSO) across Europe. The CSP working group is made up of the cyber security experts from each TSO who discuss and put together papers that can enter the standards and law of network operations across Europe. National Grid is represented on this group by the DR&S Head of Operational and Information Technology. This is the main stakeholder group of the CNI case study and will provide a forum to survey different regulatory structures across the TSOs, present working models from WP4, 5 and 6 and discuss policy papers.
Energy CISO round table			UK &US Energy industry	Adhoc meetings	The Energy CISOs round table meeting is a forum where the Chief Information Security Officers (CISOs) of Energy companies in the UK and US can exchange information, such as threats and risks, discuss issues within the industry and future concerns. National Grid chairs this group and is represented by its CISO, the Head of DR&S. This group is being utilised to brainstorm future threats and risks in the energy industry as well as discuss the policy assessments and recommendations in Deliverable D2.5.
TNCEIP	DG-Energy		EU industry	Adhoc meetings	The Thematic Network on Critical Energy Infrastructure Protection (TNCEIP) represents European owners and system operators of large scale energy infrastructure in electricity, gas and oil sectors. TNCEIP has contributed to the European Programme on Critical Infrastructure Protection (EPCIP) Directive and hopes to continue its positive involvement as the Directive is changed or updated. The TNCEIP group provides an opportunity to look at the holistic security view of the energy infrastructure at a European level (trans-border) that individual member states can benefit from. By highlighting and recommending security frameworks and controls at a European level, it makes it easier for the member states to justify these costs to their regulator when

Groups	Regulators	Gov. Agencies	Industry	Freq.	Forum of meetings / workshops & details
					approving tariffs. National Grid is represented on this group by its CISO and Head of DR&S. This group will provide valuable input to the Work Package 2 through its knowledge and position papers that look at trans-border issues and reliance that an individual member state may not fully take into account.
ENISA Smart Grid WG	All Directorates including: DG-Energy DG-Connect DG-Information	ENISA	EU industry	3-4 meetings per year	ENISA is currently heavily involved in a number of new technologies, propositions and programmes from an information security perspective. One such new technology is Smart Grid. National Grid is represented on the ENISA Smart Grid working groups by the DR&S Head of Policy, Strategy and Architecture. Whilst Smart Grid is a possible area of future risks to electricity transmission the main input to attending such working group meetings is to raise awareness of Seconomics with ENISA, the European agency that reports directly to DG-Energy. In addition, these working group meetings provide a number of opportunities to liaise with industry, particularly vendors, and peer organisations at a European level.
SCSIE		CPNI	UK industry (CNI operators)	Quarterly	The SCADA and Control Systems Information Exchange (SCSIE) is a forum facilitated by CPNI to bring together the different CNI operators in the UK to share information of all types. National Grid is represented on this forum by the DR&S Head of Investigations & Threat Management. The UK Government Agency, CPNI, facilitates this forum and advises government departments on cyber security issues. Therefore, this provides a very good forum to discuss the outcomes of the Seconomics project for the CNI case study and beyond.
STEG	DECC	CPNI	UK industry	Monthly	The GB Smart Metering Security Technical Experts Group (STEG) is a group that bring together the security experts of the GB energy industry who have an interest in the GB Smart Metering rollout. This includes energy suppliers, meter manufacturers, National Grid, CPNI and CESG. DECC facilitates the group meetings.

Groups	Regulators	Gov. Agencies	Industry	Freq.	Forum of meetings / workshops & details
					National Grid is represented on STEG by one of the DR&S Security Consultants who has a background in Smart Metering. Due to the potential Smart Metering based risks to the electrical transmission network, these meetings provide an opportunity to gather information on these risks as well as feed National Grid's assessment of these risks back into the group.
ENA			UK Energy Networks Industry	Adhoc Meetings	The Energy Networks Association (ENA) is an industry trade body that represents the transmission and distribution network operators for gas and electricity in the UK and Ireland. National Grid, as the UK electricity transmission operator, is a member of the ENA. We will utilise this membership to discuss information/cyber security issues, concerns etc. with the other industry parties. In particular, we hope to disseminate the policy papers and recommendations to them in the later phases of the project.

As shown on the stakeholder map, we have also been and will continue to engage with teams internally including:

- DR&S who ensures that National Grid, both in the UK and US are meeting the information and cyber security standards and necessary reporting to the relevant regulators
- CNI Networks teams who 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 teams who look at the future requirements of the electrical transmission network in the short, medium and long term.

Engaging with these teams is undertaken on a less formal basis but a list of major input can be found in Appendix 3 as part of the validation of this deliverable.

4. 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.

To better understand the impact of both accidental incidents and malicious attacks we will refer to the Business Impact Level (BIL) tables that were introduced in deliverable D2.2 and are presented again in Appendix 1.

4.1 Current State

As we have seen in Deliverable D2.2 there are many aspects to National Grid's CNI systems, processes and assets. The systems and assets will have different impacts to business, UK citizens, UK infrastructure and economy if they were to be compromised either accidentally or maliciously. As discussed in D2.2, we will be using the risk assessment methodology used by the UK government departments, which is specifically focused on IT systems and supporting processes that have the potential to impact the country's infrastructure, economy, international relations, defence, public services and public safety. 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'.

Figure 4 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 and identifies which parts are in scope. The oval objects represent different business services, systems and infrastructure which are referred to in the HMG IS1 methodology as 'business objects'. The rectangular objects represent services, systems and infrastructure that support the business and are referred to in the HMG IS1 methodology as 'support objects'. For example, the CNI data centres support the management of the electricity transmission network. 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.

[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

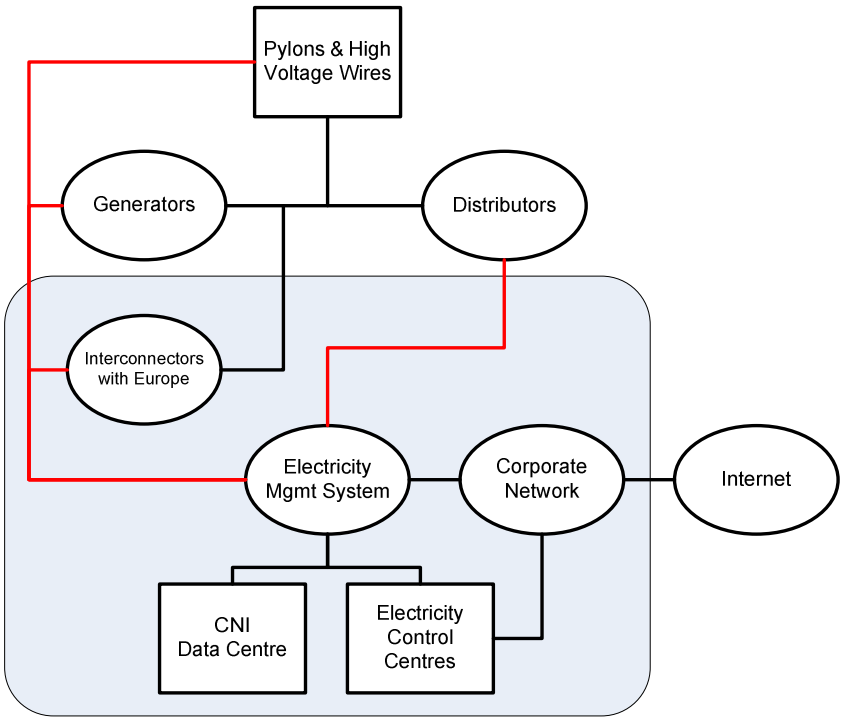

Figure 4 - Logical diagram

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

The objects presented in Figure 4 were described in Deliverable D2.2. However, a better understanding of National Grid's electricity transmission network allows us to better visualise the data and physical connections between the business objects in Figure 1, which were described in Section 2.

Following the methodology of HMG IS1 our discussion of the Current State follows a slightly different layout to that presented in Deliverable D2.2. First we will discuss the Threat Sources and Threat Actors that play a part in the Current State of the UK's electricity transmission network. We will see that 'Employees' are an important factor on all the business objects in scope and thus are discussed first. All of the information on threat actors and employees will feed the assessment of each business object.

4.1.1 Threat Sources and Actors

Deliverable D2.2 described the methodology that would be used to determine the level of threat to National Grid from different threat actors using HMG IS1 methodology. A matrix to determine threat level from levels of capability and motivation can be found in Appendix 2. The HMG IS1 methodology is quite comprehensive in its definition and explanation of threats and separates threat actors from threat sources. A threat source is a person or organisation that desires to compromise or breach security and will ultimately benefit from this activity in some way. A threat actor is a person or group who actually performs the attack or, in the case of accidents, will cause the accident.

For example a state sponsored group (threat source) may wish to bring down a country's power grid, and they may influence an employee (threat actor) within the grid operator to actually perform the attack.

Therefore, it is important to first understand the potential threat sources that may apply across the different business objects. Using a variety of sources of information, internal to National Grid and from external agencies we have presented the high level threat sources in Table 2 for each threat source we assess their level of capability and motivation as described in HMG IS1. The level of capability ranges from 1 (very little) to 5 (formidable) and each level is described in more detail in Appendix 2 Table 11. The level of motivation ranges from 1 (very low - indifferent) to 5 (very high - focussed) and each level is described in more detail in Appendix 2 Table 12. HMG IS1 provides a set of metrics for combining the level of capability and motivation to produce a threat level. These metrics are provided in Appendix 2 Table 13.

Table 2 – Threat Sources Capability, Motivation & Derived Threat Level

Threat Source	Description	Capability	Motivation	Threat Level
Foreign Intelligence Services/State Sponsored Group	Foreign Intelligence Agencies or groups that are state sponsored are considered to have resources with a variety of expertise as well as the funds to invest significant manpower to penetrating a system. Through being led by a state at the highest level, the motivation to attack an agreed target is very high and focussed. However, their motivation to attack another country's electricity transmission network using current means may have repercussions on their own state. In addition, there are far better targets which are easier to attack or easy to hide their attacks.	5	2	Substantial
Terrorist Group	Terrorist groups often have a high motivation to attack an entity such as a country's infrastructure. However, there are high value and more prominent targets than a country's electric transmission network. These groups invest time in penetrating a system either electronically or physically.	3	4	Moderate
Organised Crime	Organised Criminals are motivated by financial gain and there are limited methods to commit fraud or threaten ransom money on a country's electricity transmission network. However, opportunities exist in the wholesale electricity market and organised criminals have the capability to deploy multiple computer experts in this area for a significant period of time.	4	3	Substantial
Activists	In the current state, activist may target National Grid due to the building of towers or facilities in controversial areas	2	2	Negligible

Threat Source	Description	Capability	Motivation	Threat Level
	or as a secondary target to the building or commissioning of new power stations. Due to this, their motivation is quite low with respect to cyber security space.			
Hacktivists	Hacktivists tend to be lone computer experts spread out globally that work together to target organisations for different purposes. Hacktivists are also able to command large botnets to perform dedicated denial of service attacks. Other organisations in the UK energy sector have previously been targeted but the attacks have been limited to the defacement of their front end websites.	3	3	Moderate

These threat sources may potentially influence threat actors, through bribery, blackmail, employment etc., to penetrate or attack a system. For each business object different threat actors may be involved in attempting to compromise the system either maliciously or accidentally. Below, we describe the different threat actors that may form part of the risk assessment of the business objects presented in Figure 4.

- Employees: This threat actor group is discussed in greater detail in the next subsection.
- Commercial Partners: These organisations are ones which National Grid work with in order to fulfil its regulated duties to transmit electricity across the UK. They could include organisations operating the other ends of interconnectors in other countries, owners and operators of power generation sites or distribution network operators.
- Service Providers: These are organisations that provide National Grid systems and, more specifically, services over these systems. For example CNI communications services across the transmission network or IT services in National Grid data and control centres.
- Physical Intruder: These actors are those which attempt to attack/penetrate a system by gaining physical access to it. This may include breaking into a National Grid site such as a data centre. Also, this threat actor group may attack systems electronically or physically by destroying or sabotaging equipment. For example a physical intruder, possibly influenced by a terrorist group, may attempt to physically attack a National Grid data or control centre or even a substation using a heavy goods vehicle. Whilst such an example is a long standing physical risk unrelated in information/cyber security, such attacks will be considered in both the current and future states. In particular, there may be a lower motivation to attempt an electronic attack if a physical attack is more likely to be successful and produce a larger impact.
- Malicious Attacker: This threat actor group are those that wish to attack National Grid remotely via electronic means, social engineering etc. In particular, they are

external attackers who could be influenced by State Sponsored Groups, Terrorists or Hacktivists.

- Support Staff: We have listed Support Staff as a separate threat actor group from Physical Intruder and Malicious Attacker. Support Staff have legitimate reasons to be within National Grid sites and often are opportunistic attackers. In particular, they may have legitimate physical access to the most critical National Grid sites but do not have legitimate access to the IT systems. Examples of Support Staff include National Grid cleaners and maintenance staff.

Employee Behaviour

All of the business and support objects in Figure 4 have a people aspect to them. In particular, it is the employees of the CNI operator that can have the greatest affect on the level of threat, impact and risk to those objects.

Employee behaviour that is misaligned to the organisation can have significant effects on any organisation. Across different organisations the motivation of employees, careless or malicious, are similar although for an operator of CNI, the impact of an incident can be much larger due to the potential for disruption of electricity supply and public services.

In a generic organisation with IT systems one can categorise employees as those with elevated privileged access (privileged users) and those with "normal" access (normal 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. In the case of electricity transmission, the privileged user group includes control room users.

The small subset of employees who have the potential to cause a negative impact, in terms of information/cyber security can be put into one of four groups. These groups have different threat levels associated with them. However, the capability of all groups across normal users is considered the same. The same is the case for all groups across privileged users. In Table 3 below we give an estimation of the threat level posed by these groups of employees.

For the different business objects, different employee threat actor groups will apply and can potentially be influenced by different threat sources are described above in Table 2.

Table 3 - Threat level posed by employees

Employee Group	Description	Motivation	Normal User **Capability 3** Threat Level	Privileged User **Capability 4** Threat Level
Care-less & routine	Day-to-day violation of information security policies due to ineffective policies or lack of awareness	1	Low	Low
Care-less & business critical	In order to meet business critical needs the information security policies are circumvented	2	Low	Moderate
Disgruntled	A previously good employee who has since become unreliable due to an event such as being made redundant, a work place grievance or a change in personal circumstances	3	Moderate	Substantial

Rogue	An individual placed or targeted within an organisation with the sole purpose to attack or compromise the security of the CNI systems. Sponsored by foreign intelligence or being blackmailed or coerced in some way.	4	Moderate	Severe

As shown in Figure 4 the following business objects are in scope:

- Interconnectors
- Electricity Management System and data links with generators, distributors and interconnectors
- Corporate network and IT Infrastructure supporting Electricity Transmission.

For each business object different threat actors will be influenced in different ways by threat sources to a variety of levels. Motivations to attack the relevant business objects, as well as the capability to do so, will be different and in the following sections we will describe these influences, the different threat levels and the maximum business impact. This in turn can be translated into indicative risk levels.

Our focus will be on the generic risks to electricity transmission and we will not be taking into account vulnerabilities specific to National Grid systems, services or processes.

4.1.2 Risk Assessment – Interconnectors

The 'Interconnectors' 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 countries across Europe to utilise electricity from their neighbours in order to balance demand. Making this functionality possible allows countries to limit the amount of reserve capacity it must hold as well as help with any potential unplanned changes in demand or supply such as increases due to weather 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 flow of electricity between countries. Many interconnectors have been built across Europe. In particular, Switzerland has interconnectors with all its neighbours. Each individual country's grid operator needs to balance their respective grid(s). However, there is the added complexity that they need to meet demand or supply of electricity from the interconnectors.

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

Different countries across Europe have different levels of reliance on their interconnectors. For example, Italy relies heavily on the interconnector it shares with Switzerland. Often, the Switzerland Transmission Service Operator (TSO) takes in-feeds

from its interconnectors with France, Germany and Austria and transports that power to Italy. An example of the impact of this reliance was the previous blackout in Italy caused by its interconnectors with Switzerland (see Section 2.4).

We have assessed the business impact of a compromise of Italy's interconnector with Switzerland using the HMG IS1 Business Impact Level (BIL) Tables in Appendix 1 and this is presented in Table 4. This has been completed in terms of the following attributes as described below:

- Confidentiality of the data flowing across the data link at the interconnectors
- Integrity of the data flowing across the data link at the interconnectors
- Availability of the data flowing across the data link at the interconnectors.

Table 4 – Impact assessment of Italian/Swiss Interconnector

Security Attribute	BIL	Assessment
Confidentiality	2	See Appendix 4A for a detailed assessment
Integrity	5	See Appendix 4A for a detailed assessment
Availability	4	See Appendix 4A for a detailed assessment

The UK has two interconnectors which are frequently used to import electricity rather than export. This is due to the price of the electricity from the Netherlands and France tending to be lower than that of electricity produced in the UK. Therefore, there is not a large 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 not be significant. Given this, we have assessed the business impact of the UK interconnectors with France and the Netherlands, in a similar way to the Italian/Swiss interconnector, which is presented below in Table 5.

Table 5 – Impact assessment of UK Interconnectors with France and the Netherlands

Security Attribute	BIL	Assessment
Confidentiality	2	See Appendix 4A for a detailed assessment
Integrity	3	See Appendix 4A for a detailed assessment
Availability	3	See Appendix 4A for a detailed assessment

Taking the threat sources assessed in Section 4.1.1 as well as the standard set of threat actors identified, a threat assessment of interconnectors is presented in Appendix 4A. We have applied this threat assessment to both the UK interconnectors and the Italian/Swiss interconnector impact levels (Tables 4 and 5 respectively) to produce an indicative set of risk levels. It must be noted that the risks identified are generic, as they do not take into account vulnerabilities specific to particular IT systems or business processes.

Each threat actor could attack different attributes of the systems, in particular its confidentiality, integrity or availability. Using our source information, different threat actors may only be motivated to attack certain attributes of the system and this is presented in the assessment. Also each threat actor, for the different attributes, may be

influenced by a threat source to undertake the attack. This means that the capability and motivation of the threat actor are heavily influenced by those figures of the threat source. However, this does not mean that the threat actor takes the exact value of the influencing threat source's capability and motivation. For example, if a threat actor is influenced by Foreign Intelligence/State Sponsored Groups (capability: 5 and motivation: 5) this does not mean the threat actor automatically gets those levels of capability and motivation as the State Sponsored Group may not be overly motivated to attack this particular system through that particular threat actor.

In addition, we have only included the privileged user employee groups (control room employees, system administrators etc.) as this threat is more significant than the normal user employee groups.

4.1.3 Risk Assessment – The Electricity Management System and Data links with Generators, Distributors and Interconnectors

In the Further Background, Section 2, we described how the Electricity Management Systems (EMS) manages the electricity transmission network through exchanging information with the electricity generators, the distributors, the interconnectors. Also, we looked at how the SCADA systems brings together information from throughout the physical assets across the grid including

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

This information is critical for the correct management and 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.

When we assess the business impacts, threats and risks for the EMS and its associated data links we are also considering the IT infrastructure that makes up these systems. Current government guidelines suggest/mandate additional physical and information/cyber security measures should/must be implemented to ensure the protection of the CNI systems (i.e. EMS) over and above standard IT infrastructure. In, Section 4.1.5 we will look at the IT infrastructure that supports the National Grid corporate network.

As in the previous section we have assessed the business impact of the EMS and its associated data links using the HMG IS1 Business Impact Level (BIL) Tables in Appendix 1. This has been completed in terms of confidentiality, integrity and availability as described in the previous section.

Table 6 – Impact assessment of the EMS and Data Links with Generators, Distributors & Interconnectors

Security Attribute	BIL	Assessment
Confidentiality	2	See Appendix 4B for a detailed assessment
Integrity	5	See Appendix 4B for a detailed assessment
Availability	4	See Appendix 4B for a detailed assessment

Taking the threat sources assessed in Section 4.1.1 as well as the standard set of threat actors identified, a threat assessment of the EMS and its data links with generators, distributors and interconnectors is presented in Appendix 4B. We have applied this threat assessment to impact levels in Table 6 to produce an indicative set of risk levels. It must be noted that the risks identified are generic, as they do not take into account vulnerabilities specific to particular IT systems or business processes.

4.1.4 Risk Assessment - Corporate Network and IT infrastructure supporting Electricity Transmission

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 as an identified provider of CNI, an additional dimension has to be considered when developing and implementing the corporate IT architecture.

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

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

The challenge for the grid operator is to interconnect securely and reliably 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.

With this in mind, and as in the previous sections, we have assessed the business impact of National Grid's corporate network using the HMG IS1 Business Impact Level (BIL) Tables in Appendix 1. This has been completed in terms of confidentiality, integrity and availability as described in the previous section.

Table 7 – Impact assessment of the Corporate Network and IT Infrastructure supporting Electricity Transmission

Security Attribute	BIL	Assessment
Confidentiality	3	See Appendix 4C for a detailed assessment
Integrity	3	See Appendix 4C for a detailed assessment
Availability	2	See Appendix 4C for a detailed assessment

Taking the threat sources assessed in Section 4.1.1 as well as the standard set of threat actors identified, a threat assessment of National Grid's corporate network is presented in Appendix 4C. We have applied this threat assessment to impact levels in Table 7 to produce an indicative set of risk levels. It must be noted that the risks identified are generic, as they do not take into account vulnerabilities specific to particular IT systems or business processes.

4.2 Future State

In Section 4.1 we described and assessed the security impact, threats and risks of the key areas of the Current State of National Grid's electricity transmission network in the UK. In this section we discuss the possible Future States of electricity transmission in the UK. 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.

Unlike the current state, as there are many unknowns, it is more difficult to perform a technical threat and risk assessment as was performed on the different business objects in Sections 4.1.2, 4.1.3 and 4.1.4. Instead, following various roundtable discussions internally with the Digital Risk & Security Team leads and with other Energy Company CISOs in the UK and US we will look at the potential Future State through a number of lenses. The four lenses are:

Impact: Has the fundamental purpose of the business objects altered so that their business impact, in terms of confidentiality, integrity and availability, has changed? The reliance on electricity by a country's citizens, companies, institutions and government has never been higher and it can be reasonably hypothesised that this reliance will increase in the future. However, in terms of the HMG IS1 business impact level we have made the assumption that, in the medium term, these levels will not increase. This assumption allows us to measure the changes to the risk through the other lenses against the Current State more accurately.

Opportunity: Has there been an increase in functionality of the business object, the introduction of new technology or has innovation changed the opportunity for attackers to compromise the particular system? In information/cyber security, opportunity is often referred to as the 'attack surface'. If the attack surface has increased this may mean that there is a higher likelihood of an attack as there are more attack vectors. In terms of the HMG IS1 framework this is captured as an increase in the motivation for attackers

leading towards a possible increase in their capability as the system may now be more vulnerable to attack. A simple (unrealistic) example would be if the EMS infrastructure became directly connected to the internet. This would dramatically increase the attack surface or opportunity to attack the system. The capability of the threats for this business object would significantly increase due to the tools and attack methods which could be implemented across the internet.

Threat Sources/Actors & Motives: In the future the current set of threat sources and actors may have a different level of motivation to attack the systems, perhaps due to a change in Opportunity. In addition, there may be new threat sources and actors that implicitly or explicitly wish to attack the systems.

Means: New technology and innovation may provide new means for threat actors (influenced by threat sources) to successfully attack the business objects. In terms of the HMG IS1 framework this is captured as an increase in the threat's capability. As described under the Opportunity heading, the change in the Means may be as a result of a change in the attack surface thus changing the capability for an attacker to successfully attack the system.

In the next sections we consider possible Future States through these lenses and from this we can build a picture of the future and emerging threats, opportunity and indicative risk.

4.2.1 Opportunity

We will look at the opportunities in the future state of the Interconnectors, EMS and its data links to the generators, distributors and interconnectors and the Corporate Network under separate headings. Also, a new area of opportunity that will affect all citizens in Great Britain is the nationwide rollout of Smart Meters. Due to its significance and that it has the potential to affect all areas of the future state, we have discussed Smart Metering under a separate heading.

Interconnectors

New electricity interconnectors are planned between the UK and other countries across Europe such as Norway and Denmark. In addition, more functionality may be added to these and current interconnectors with France and the Netherlands to allow commands to be sent electronically (within contractually agreed parameters) to the TSO at the opposite end of the interconnector.

The capability to send commands to the opposing end of an interconnector means that National Grid would become reliant upon the cyber security status of the opposing TSO. By extending the management and control capability, and increasing the number of interconnectors, the attack surface will expand raising the risk that malware, hacks and other malicious attacks can penetrate the core UK CNI.

The Electricity Management System and Data Links with Generators, Distributors and Interconnectors

National Grid foresees a number of areas of new technology and innovation that could increase the attack surface on the electricity management system and its data links in the future.

- **'Command and Request' data links**: Data links between the SCADA systems and generators/distributors may become automated 'command and request' links rather than just request links, in a similar way to the Electronic Highway. Generators and distributors will be reliant upon the security of National Grid's system in order to trust these commands to ramp up/down the generation at a particular site or shut off particular distribution zones. There is more opportunity to cause an impact on the electricity transmission network via the interception of these command messages.
- **Combination of IT and Operational Technology**: Operational technology (OT) increasingly relies on embedded IT to function and IP communications to support remote control. This trend is expected to continue placing an increased responsibility on these systems to be patched to maintain security. In addition, these complex systems require maintenance engineers to use mobile computing devices and software applications to support and configure activities. This extends the traditional IT security perimeter and increases the cyber vulnerability of the CNI. This in turn increases reliance on physical security and monitoring.
- **Confusion of complexity**: The trend towards more intelligence embedded within OT environment and SCADA systems has increased the functionality and complexity of the whole CNI command and control environment. This has created the potential for new vulnerabilities in application software, firmware or other source code. Security assurance during software development and system deployment will become increasingly important. Due to increasingly complicated functionality or code, verification and accreditation becomes increasingly difficult and/or less effective. The impact could be that business applications or systems (including SCADA systems) have malicious code within them. Utility trading, transmission or distribution could be affected with potentially grave impacts.
- **Procurement and Commoditisation**: In the future, continued drive towards increasing commodity prices may lead to lower assurance and vulnerable commercial-off-the-shelf (COTS) technology, including SCADA and transmission equipment, being used in the enterprise. Greater use of outsource providers causes this risk to be one step removed from security assurance processes and therefore completely out of sight of the company. Also, this leads to increasing difficulty in specifying security controls to be used and assuring and monitoring them, particularly with a changing threat environment. Therefore, there is potential for future vulnerabilities to materialise that the company is not prepared for.

Corporate Network

All large organisations have to deal with similar security issues across their corporate networks, however, for companies that operate CNI these issues have potentially higher impact. Below, we consider the opportunities that could increase the attack surface across the corporate network some of which may have an impact on our CNI systems.

- **More complex electricity management systems**: National Grid's business may require more extensive links between the corporate network and the CNI SCADA systems. This may result in interfaces between the CNI SCADA systems and the

internet. This opens the CNI systems and equipment to a vast array of attacker and attack methods which the systems have not been built to defend against.

- **Bring-your-own-IT (BYOIT):** The ever changing digital lifestyle is driving the use of low assurance devices for high assurance operations within a corporate network linked to CNI operations. There are potential legal challenges in securing devices that the organisation does not own. It will continue to be ever more difficult for an organisation to keep abreast of the functionality of consumer devices and thus 'locking them down' to an acceptable level of assurance will also continue to become ever more difficult.
- **Social Media**: Organisations across many industries are using social media for various purposes. Therefore in the future, it is possible that CNI operators could start to use social media for sensitive subject areas such as engineering support. This could inadvertently release sensitive/important information which is helpful to attackers. For example, there have already been tensions within National Grid over the publishing of utility pipeline maps for safety purposes versus withholding them for security reasons. With the use of social media for more sensitive purposes, identity and access management will become more difficult to control e.g. passwords and IDs appearing outside of the enterprise.

Nationwide rollout of Smart Meters in Great Britain

Following a European Directive, the UK government is currently in the initial phases of rolling out Smart Meters to homes in England, Wales and Scotland. The rollout of Smart Meters has the potential to affect different areas of National Grid's business affecting interconnectors, the EMS and its data links and the Corporate Network.

The Smart Meters will include switches, to turn the supply of electricity off or on, that are remotely controllable by the customer's energy supplier. A mass compromise of Smart Meters which are switched off then on continuously could cause frequency spikes on the electricity transmission network. This in turn could cause power stations to trip and blackouts across the country. Smart Meters present an opportunity for attackers to target the electricity transmission network through devices in relatively insecure environments. In addition, Smart Meters and the risks they bring may require more complicated and automated algorithms to balance the electricity grid. This may result in knowledge gaps in personnel and more reliance on computers to balance the grid.

The balancing and settlement of the wholesale energy market is completed on the Corporate Network using averaged and estimated demand profile information which is not accurate. In the future, once Smart Meters have been fully rolled out, it is envisaged that wholesale settlement could be made more accurate using the accurate energy usage from a sample, if not all, Smart Meters. This creates potential privacy concerns if National Grid is handling energy usage information from households for settlement. Attackers may directly, or through influencing staff, steal the energy usage data and sell it to companies on the black market.

4.2.2 Means

Before considering the threat sources and actors for the Future State, it will first be useful to look at the means available to attackers in the Future State. This will feed into the capability of the threat sources. Below we give an overview of the new means

following various roundtable discussions internally with the Digital Risk & Security Team leads and other Energy Company CISOs in the UK and US:

- **Advanced Malware**: With the arrival of bespoke malware such as Stuxnet and Flame, as described in Section 2.5, organisations could finance advanced malware building teams (perhaps run by criminal organisations) to build the next bespoke malware. The effect of such malware being deployed could be a major impact to CNI operators that are targeted.
- **Commodity Cyber Weapons**: Security researchers may see attacks for research purposes as not being unethical and as a consequence build easy to use attack tools in the public domain. Mobile platforms, such as mobile device operating systems, may become the next easy to attack platform with script kiddie tools etc.
- **Quantum computing or easy access to cloud grid computing**: This may open up cryptographic attack to low budget attacker increasing the likelihood of attack. For example, key cryptographic protocols such as SSL, become untrustworthy due to new publicised attacks. This may be of particular issue to long-life assets and technology (i.e. those used in CNI systems) with limited scope to upgrade.
- **Technical Back doors in IT equipment or software**: This may become a problem of COTS with built-in backdoors, especially low cost COTS equipment or software. For example attackers may routinely take advantage of imbedded malware in base/core elements of computer devices, such as integrated circuits contaminated with malware.

These new means of attack may be used by threat actors, through influence by certain threat sources, in the Future State. By putting together the new opportunities (increase in levels of motivation and attack surface) and the new means (increase in levels of capability) we present a high level threat assessment for the Future State in a similar way to that completed in the Current State in Section 4.1.

4.2.3 Threat Sources/Actors & Motives

In the Future State, the new opportunities to attack the Interconnectors, EMS and the corporate network may introduce new threat sources/actors as well as change the motivation level of the current threat sources. The new means of attack may increase the capability of these threat sources/actors. In Table 8[2] below, we present a threat assessment for the Future State based on the information in the earlier sections.

[2] In the Future State, the way in which employees work such as their dependence on new digital technology and social media may change (increased dependence). Employee loyalty may decrease within CNI operators as it has done in other sectors such as the financial sector. National Grid is of the view that whilst these changes may affect the levels of capability and motivation of the employee set of threat actors, the most extreme threat of rogue employee (Threat Level: Severe) will not change.

Table 8 – Future State - Threat Sources Capability, Motivation & Derived Threat Level

Threat Source	Description	Capability	Motivation	New Threat Level	Previous Threat Level
Foreign Intelligence / State Sponsored Group	In the future state, the increased opportunities (e.g. smart metering and command and request data links) to attack a country's electricity transmission network remotely (e.g. advanced malware, cyber weapons), perhaps for cyber warfare, allow the threat actors to remain hidden. Therefore, the electricity transmission network may become a higher priority target for such groups. In addition, in the future greater numbers of smaller nation states will gain the capability and sophistication to build cyber attack tools and weapons. These groups may well be less discriminating on how they test and deploy attacks whether deliberately or accidentally. Alternatively, Foreign Intelligence as part of international business or deliberately for espionage purposes may buy utility companies which will gives them access to inside working knowledge and information sources of the industry and even a 'test bed' for attack modelling. This restricts the ability of government agencies to share sensitive information freely in the industry (potentially creating some weakest links) and also acts as a barrier to improved information sharing which could even fail because of lack of sufficient trust of other players.	5	***5***	**Critical**	Substantial
Terrorist Group	In the future, there is potential for Terrorist groups to recruit more IT proficient people to their causes. As the impact , either actual or perceived, of attacking information assets increases Terrorists may wish to invest more time into attacking targets from an information or cyber aspect. They are likely to be more privateers or terrorist but may be performing permitted activity by a state even if not state sponsored.	***4***	4	**Severe**	Moderate
Organised Crime	Organised Criminals are motivated by financial gain and there are limited methods to commit fraud or threaten ransom money on a country's electricity transmission network. However, opportunities exist in the wholesale electricity market and organised criminals have the capability to deploy multiple computer experts in this area for a significant period of time.	4	3	**Substantial**	Substantial
Activists	There are numerous projects and programmes that National Grid may become involved in that	2	***3***	**Low**	Negligible

Threat Source	Description	Capability	Motivation	New Threat Level	Previous Threat Level
	have the potential to incite activism. For example, the building of new or replacement nuclear power stations and installation of wind farms onshore. Activists could include pressure groups, protest groups or simply those that fall in the category of 'Not in my back yard' (Nimbys). Activists may target these sites directly but in the future may collaborate and target National Grid via social networks, Dedicated DOS attacks or other cyber attacks to cause reputational damage.				
Hacktivists	Hacktivists are currently small groups of individuals utilising botnets to perform Dedicated DOS attacks on or defacing the front end websites of organisations or corporations that they wish to target. In the future hackers will, most likely, increase in number globally and in the UK. They will be able to call upon larger botnets, some of which may be 'willing' botnets rather than simply compromised PCs. Hacktivists may also start targeting more corporate focussed websites that link to backend databases (e.g. by technical backdoors). Corporate databases could be knocked over reducing availability or data could be stolen or corrupted. Smart Meters also present a significant opportunity to hackers to commit fraud and other activities. A targeted attack on many smart meters may affect National Grid and the electricity transmission network.	***4***	3	**Substantial**	Moderate
Security Researchers	Security Researchers in the Current State have not focussed on attacking live systems. However, in the future it is expected that the number of researchers in information/cyber security will continue to increase. These researchers may be funded through academic institutions, large corporations or by state sponsored groups. Greater numbers of smaller nation states will gain capability and sophistication in the area of information/cyber security. Security researchers within these groups may well be less discriminating on how they test and deploy attacks. In addition, academic institutions may start to feel that publishing attack proof of concepts and codes is not unethical. However, malicious attackers may use these to launch an attack on live systems.	4	2	**Moderate**	N/A

Threat Source	Description	Capability	Motivation	New Threat Level	Previous Threat Level
Inappropriate Regulation	Incorrectly or inappropriately designed regulatory structures may have a negative impact on the level of security within CNI operators. For example, the actions of other sector participants, such as the abuse of privacy of individuals from bulk data collected, could result in "knee-jerk" Regulatory intervention. This may require CNI operators to turn off functions that would be of commercial value or waste capital expenditure on unnecessary security controls. In addition, such regulatory intervention has the potential to drive all organisations to use the same controls thus any new or unforeseen risk would become systemic. Note: In the case of inappropriate regulation, we have not assigned a capability and motivation level but have instead set a threat level directly	N/A	N/A	**Moderate**	N/A

4.3 Risk Mitigation & Regulation

Having discussed the high level risk to National Grid's CNI systems, network and corporate network in the Current State and the future and emerging threats, the next step it to understand how to mitigate these risks.

Any organisation is motivated to protect itself against the security risks that it has identified as having a potential impact on its business. However, the key consideration here is that the impact of a breach on a CNI operator can have an impact far beyond the organisation itself. As we have seen above, in the case of National Grid the potential impact is BIL5 which could mean (see Appendix 1):

- Loss of power in a region of the country causing disruption for more than 1 week
- Loss of power nationally causing disruption for up to 1 day
- Severe losses to the country's business in the billions of pounds
- National disruption to the distribution of essential goods, fuel, raw materials, medicines and food for up to a month.

These impacts go far beyond National Grid itself. The issue for governments and regulators is how best to ensure such risks to CNI and their operators are appropriately mitigated. In other words, how can the CNI operators be incentivised to mitigate the risks that can have an impact beyond their organisation?

In the next section we begin to look at how regulation can be used to meet these aims, the options available and the challenges. Working closely with the other project

partners, during the course of the SECONOMICS project, we aim to provide recommendations as to which regulatory structures would work best in the CNI environment. This will be achieved through assessing them with rigorous economic and mathematically modelling tools as well as practically.

5. Policy and Regulatory Structures

In Deliverable D2.2 we began to look at the different types of regulatory structures that apply to National Grid is practice but could also apply, theoretically, to a general CNI operator. In particular we discussed:

1. two different high-level approaches to regulation applying to organisations operating critical infrastructure namely risk/principles-based and rules-based regulatory structures
2. how one can assess the usefulness and efficiency of the different regulatory structures
3. incentives of agents and how they can be modelled in the different types of regulation
4. the role of public policy in attempting to create or erode the incentives to effectively manage risks.

In Deliverable D2.2 points 3 and 4 provided an introduction to WP6 and the first deliverable in that work package (D6.1) begins to go into much greater detail in these areas.

In this deliverable point 1 is discussed in much greater detail. In particular, National Grid operates CNI in countries (UK & US) where these two contrasting approaches to regulation are implemented. Thus, we continue the discussion of point 1 above by detailing the application of the risk/principles-based regulatory structure for CNI in the UK as well as the rules-based regulatory structure for CNI in the US. Through this discussion of the two contrasting regulatory structures and the examples of how they apply to National Grid, we begin to assess their usefulness and efficiency in detail (point 2 above). This assessment will be continued in WP6.

Also, WP5 will look at building security risk models based on the information in the case study background as well as the threats and risk assessments of the current and future state. Both work packages (5 and 6) will look at the more theoretical aspects of public policy using their different methodologies and we will aim to validate these models in the next stage of the SECONOMICS project.

5.1 Risk/Principles- vs. Rules-Based Regulatory Structures

At a high level, rules are sets of instructions with either a dichotomous (adhered to or not adhered to) or continuous (10%, 20%,…, 90%) compliance measure. Principles, on the other hand, 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 may go to the next level of detail 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 of Deliverable D2.2 and utilised in the Current and Future State risk assessments[3] 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.

As explained, National Grid own and operate CNI in both the UK and US. In particular, National Grid operates electricity transmission networks in the UK and US but have to comply with different regulation in each country. In the UK, National Grid operates in a risks/principles-based environment whereas, in the US, National Grid operates in a rules-based environment. This is shown diagrammatically in Figure 5 below.

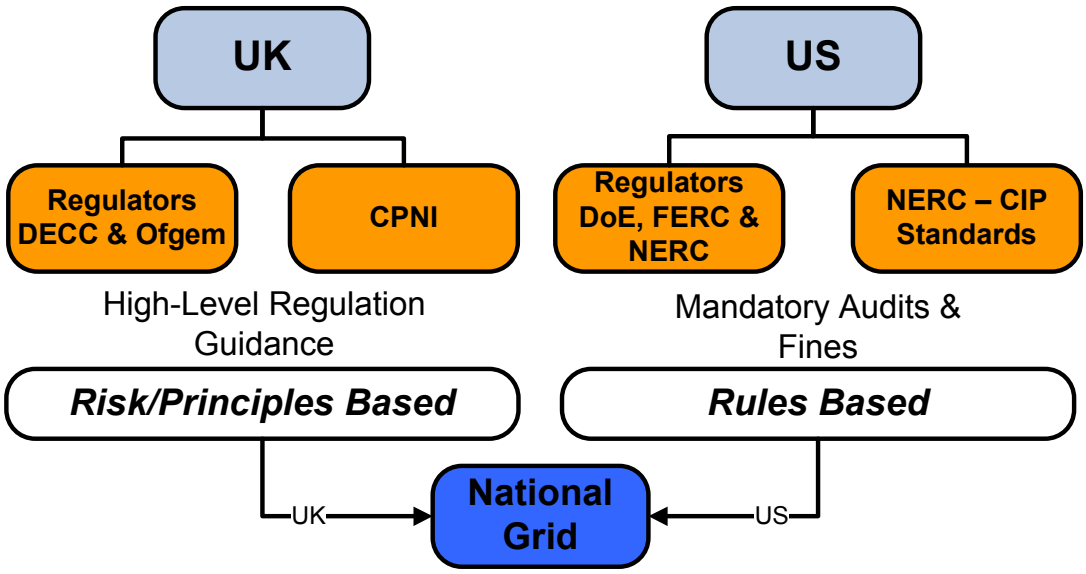

Figure 5 – National Grid Regulation in the US and UK

In the following subsections we describe these different regulatory structures in more detail.

5.2 UK CNI Regulatory Structure: Risk/Principles-Based

In the UK the Department for Energy and Climate Change (DECC) is responsible for ensuring the security of supply of energy i.e. there is enough electricity generation

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

capability for the long term future of the UK. This includes power generation, energy transmission, energy distribution and supply to the 'last mile'. DECC is led by a government minister.

The responsibility of regulating the energy markets in England, Scotland and Wales is independent of government and it instead given to a quasi-governmental organisation, the Office for Gas and Electricity Markets (Ofgem). This ensures that energy regulation is free from political interference, and helps avoid uncertainty in energy markets. Ofgem's key functions include:

- issuing, modifying, enforcing and revoking licenses
- setting price controls in the natural monopoly licensed sectors
- investigating and penalising those in breach of licence conditions.

We will look at how Ofgem regulates prices in the power delivery chain and how that affects corporate investment such as in information security.

5.2.1 UK Electricity Energy Market

The market of energy, including electricity, is monopolistic in nature. There will only be one set of wires and cables linking the power generation sites to households and non-domestic sites (via a variety of substations). Therefore, whilst different parts of the power delivery chain can be made the remit of different organisations, as there is only one set of cables the market is monopolistic. In the UK, to encourage competition in the energy market, the supply of energy can be considered as a service where the electricity delivered to a household is the same regardless of the service provider. To facilitate this, other organisations are in charge of running the electricity market to ensure that demand is met and that the cost is correctly recharged to the relevant energy supplier. These organisations are:

- Gemserv: own and operate the database of electricity metering points in the UK. This database is used to maintain and manage the meters in households and non-domestic premises and is essential when a premise goes through a change of energy supplier.
- Elexon: operate the half-hourly wholesale electricity market. Part of their role is to accurately distribute the cost of electricity supplied by power generation sites to the energy suppliers that have demanded electricity for their customers.
- Electralink: manage the Data Transfer Network which is a dedicated communication network, linking all organisations that are involved in the energy industry. This network helps facilitates the wholesale electricity market.

For electricity to be delivered to UK households the following types of organisations are essential:

- Power generators: There are six types of generation sites in the UK including nuclear, coal-fired, gas-fired, hydro, solar and wind.
- Electricity Transmission: As discussed, this is the remit of National Grid who own and operate the electricity transmission grid.
- Electricity Distribution: The UK is split into 14 distribution regions which are individually franchised or leased to companies referred to as Distribution Network

Operators (DNOs) who are the sole provider of electricity distribution in that region.

- Energy Suppliers: These companies interact directly with the customer or end user of electricity whether they are an individual, small or medium sized enterprise, factory or other commercial site.

Having described the UK electricity market at a high level, we will see how Ofgem regulates the market and focus on the effect on security of this regulation.

5.2.2 UK Regulation

The only organisation in the power delivery chain that the end user has a relationship with is the energy supplier. Thus all costs for power generation, transmission and distribution are included in the energy supplier's bill to the end user. Whilst the UK energy market is considered the most competitive in the world, only the sectors of energy suppliers and power generation are competitive. The other areas, by their very nature, are monopolistic and so the prices charged to consumers for generation, transmission and distribution are heavily regulated by Ofgem. In addition, Ofgem regulates the amount of profit, and thus prices, that the energy suppliers can charge consumers.

In electricity transmission, Ofgem's key role is setting price controls on how much National Grid can recover its costs from the DNO's which is then transferred to the end consumer through the energy suppliers. For Ofgem and National Grid to understand how much can be charged, it is essential that the current and future costs, both operational and investments are known. Information and cyber security is critical to the safe operation of the transmission network and, thus, is a cost to the business. Ofgem then judge whether these costs are justified and can be charged to the energy consumer.

The Centre for the Protection of National Infrastructure (CPNI), a government agency, has the technical skills to understand the different security policies and controls that an operator of CNI should implement. CPNI provide guidance and protective security advice to government departments and to providers of CNI directly. Ofgem and DECC are able to get advice from CPNI around the controls, costs and investment that are justified by a provider of CNI, such as National Grid.

CPNI offer lines of communication and information exchange forums for owners and operators of CNI. In addition, CPNI chairs and attends cyber security meetings for CNI providers. For example, CPNI chair and coordinate the 'SCADA and Control Systems Information Exchange' (SCSIE) where providers of CNI (including National Grid) attend and exchange information on current and future threats, vulnerabilities and risks. In addition, CPNI produce and disseminate guidance on operating CNI. For example, they produce guidance material on SCADA covering the following areas:

- Understanding the business risk of SCADA
- Implementing secure architecture
- Firewall deployment for SCADA and process control networks
- Establishing response capabilities
- Improving awareness and skills
- Managing third party risk

- Engaging with projects throughout the life of the SCADA
- Establishing ongoing governance.

To make this guidance accessible to operators of CNI, they have also produced a SCADA Self Assessment Tool (SSAT) in line with each domain of information security, which can be completed against each CNI system annually. The important point to emphasise with all this information and tools is that they are guidance. There is no mandatory or regulatory requirement for a CNI operator to take account of the guidance and to complete the SSATs for each of their CNI systems.

National Grid holds the licence for transmitting electricity in Great Britain[4]. The existence of this licence and the licence holders duties and responsibilities are laid out in the Electricity Act 1989[5] and its subsequent revisions. In this piece of UK legislation, within the 'General duties of licence holders', section 9.2 states that

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

This act also requires that the electricity transmission licence holder must adhere to the electricity transmission licence standard conditions[6]. There are many standard conditions detailing the different areas where there are mandatory requirements on the transmission licence holder.

Even though the Electricity Act does not specifically require the transmission licence holder to be "secure" one could argue that not having the relevant information security controls in place could jeopardise the efficient, co-ordinated and economical system of electricity transmission. Therefore, there are a number of possible options if a CNI operator does not follow CPNI's guidance on security. Primarily, there is an implicit threat that if a CNI operator does not follow CPNI guidance, or at the very least be seen to follow CPNI guidance, the UK regulator may impose specific legislation around security. In particular, only government could impose legislation around security on the CNI operators, that is mandatory and will have the relevant clauses of noncompliance such as fines, criminal proceedings etc. Alternatively, the current legislation may be used to invoke one of the following actions:

- The regulator could sue the CNI operator under breach of legislation and a judge would make a decision based on evidence presented.
- Mandatory arbitration: This is where an independent arbitrator makes a judgement whether there has been noncompliance with the legislation around security. If the CNI operator disagrees they could appeal the arbitrator's decision in a court of law.

[4] There are some subtleties around the transmission of electricity in Scotland but for this document we summarise National Grid's role as electricity transmission licence holder for all of Great Britain including England, Wales and Scotland.
[5] Electricity Act of 1989 in Great Britain and its revisions by Her Majesty's Government.
[6] Electricity Transmission Licence: Standard Conditions by Her Majesty's Government Legislation which was updated and consolidated in April 2012.

- Contractual arbitration: This is similar to mandatory arbitration but if the CNI operator disagrees with the independent arbitrator's decision if would mean a breach of contract.

National Grid's view, up to and including board level, is to ensure we are following security best practice. To this end, National Grid chooses to follow CPNI guidance by completing the SSATs for each of the information technology CNI systems that it operates, annually. National Grid attends information exchange forums led by CPNI as this benefits the business by providing security input, for example new security threats. In addition, it builds upon the established relationship with CPNI and other CNI operators. The established relationship with CPNI keeps lines of communication open if issues or incidents do occur.

5.3 US CNI Regulatory Structure: Rules-Based

In the US, the Secretary of Energy is responsible for the Department of Energy, which is a cabinet-level department in the US Government. The Department of Energy (DoE) in the US has similar responsibilities to that of DECC in the UK. The aim of the DoE is to ensure America's security and prosperity by addressing its energy, environmental and nuclear challenges through transformative science and technology solutions.

Separately a US Federal Agency, independent of the DoE, called the Federal Energy Regulatory Commission (FERC) has jurisdiction over a number of areas[7] including:

- interstate electricity sales
- wholesale electric rates
- hydroelectric licensing
- natural gas pricing
- oil pipeline rates.

The US Energy Policy act of 2005 expanded FERC's authority to include the setting of mandatory reliability standards on gas and electricity transmission operators. These standards could be enforced with FERC's ability to impose penalties on entities that attempted to manipulate the market.

The focus here is on the reliability of the transmission systems and for electricity, FERC has the ability to grant an organisation with the status of being the Electricity Reliability Organisation (ERO). Since 2007, the North American Electric Reliability Corporation (NERC) has been the ERO for the US. NERC has the legal authority to enforce reliability standards on electricity transmission operators in the US and this includes National Grid.

NERC is an independent organisation that provides guidelines and standards 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).

There are a number of reliability standards that NERC has the responsibility of enforcing. These are listed below:

[7] Federal Energy Regulatory Commission website https://www.ferc.gov/about/overview.asp

- Resource and Demand Balancing
- Communications
- Critical Infrastructure Protection
- Emergency Preparedness and Operations
- Facilities Design, Connections and Maintenance
- Interchange Scheduling and Coordination
- Interconnection Reliability Operations and Coordination
- Modelling, Data and Analysis
- Nuclear
- Personal Performance, Training and Qualifications
- Protection and Control
- Transmission Operations
- Transmission Planning
- Voltage and Reactive.

The standard which focuses on information/cyber security as well as the CNI aspects of electricity transmission is the Critical Infrastructure Protection (CIP) reliability standard.

5.3.1 NERC CIP

The NERC CIP reliability standards provide rules for bulk energy delivery providers on securing critical infrastructure. There are a number of CIP reliability standards covering a variety of areas in information/cyber security 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.

CNI operators that have undertaken adoption of the standards need to identify there 'Critical Cyber Assets', these in turn must comply with the current standard of NERC CIP against those assets. The current standard is version 3 (NERC CIP v3).

Version 4 of NERC CIP (NERC CIP v4) was approved by FERC on 19th April 2012. FERC requires NERC to have fully implemented the compliance of CNI operators to NERC CIP v4 by 31st March 2013. NERC CIP v4 at a high level will include requirements on Network Access Control. In addition, and more specifically, there is a significant change between version 3 and 4 of the CIP-002 standard around critical cyber asset identification. In version 3, there is a risk-based assessment methodology that CNI operators must follow to identify their cyber assets. However, in version 4, there are specific criteria that CNI operators must use to identify critical cyber assets. This set of criteria is called the Bright Line Criteria. There are 17 separate critical asset criteria that apply to generating units, transmission lines and control centres. It is expected that following the

introduction of this new criteria more assets will be identified as critical and thus more effort will be required, by CNI operators, to comply with the NERC CIP standards.

Version 5 of NERC CIP (NERC CIP v5) is currently being produced by NERC. This is planned to become live in January 2015. It is expected that NERC CIP v5 will be more comprehensive and potentially prescriptive than previous versions and there has been push back by CNI operators. The key question which forms the basis of their reluctance to accept a more prescriptive standard, is how the costs to the business of compliance will be recovered through their revenue streams. As their businesses are heavily price regulated, CNI operators are expecting that future prices will take into account the extra costs of complying with more onerous standards.

5.3.2 Compliance to NERC CIP

To enforce reliability standards effectively, NERC utilises a number of regional councils throughout the US. These councils are called upon to complete audits and inspections of the transmission operators. In the north eastern states of the US, where National Grid is the transmission operator, the Northeast Power Coordinating Council (NPCC) is the regional council.

There are 171 requirements within the current NERC CIP standards which National Grid must adhere to annually. To show compliance, the NERC CIP standards require a CNI operator to complete quarterly management reviews, yearly self-certifications and an external audit by the regional council every three years. All audits, self-certifications and supporting documentation have to be stored in a Document and Knowledge Management System (DKMS). The internal and external audits as well as the production of the supporting documentation require significant effort and attention. In addition, there are daily operations that are necessary due to the NERC CIP requirements. National Grid has estimated that for each set of CNI that must comply with NERC CIP standards requires 3 full time employees solely for dealing with the compliance, documentation and other administration of NERC CIP. Due to limited budgets and cost constraints often applied from price regulation this can constrain other essential activities such as longer term and security strategy planning.

5.3.3 Areas of benefit and concern

There are both advantages and disadvantages to a CNI operator in having to comply with the NERC CIP standards. First we describe a couple of advantages or benefits of having to comply with the NERC CIP standards:

- Through the requirement on CNI operators having to comply with the NERC CIP standards, it sets a minimum level of security across all the operators. Therefore, government, regulators and citizens can be assured that there is a minimum level of security across all CNI operators.
- Currently, NERC CIP v3 contains a set of 45 high level requirement areas with more detailed requirements underneath, some of which cover implementation of those requirements. However, the level of these requirements means that they can apply to different CNI operators in different ways. Thus, there are different ways in which CNI operators can meet a requirement which gives the CNI operators flexibility in implementation and thus in compliance.

On the other hand, National Grid's electricity transmission business in the US has come across various obstacles, concerns and issues. A number of those have been described below:

- NERC CIP requires that operators of critical assets adhere to their own policies and standards. Thus if an operators standards are set at a higher bar than the NERC CIP standards the operators must adhere to their more stringent requirements. This then presents a potential concern that NERC can fine an operator if it fails to meet its own policies and standards even if the operator is within the minimum standard set out in NERC CIP. This situation provides no incentive for a CNI operator to set their policies or standards above the minimum bar set by NERC CIP.
- To reduce costs of complying with NERC CIP, operations personnel can be utilised to help with compliance work internally as they are subject matter expertise in the critical cyber assets. As a result this can create a conflict of interest with employees 'marking their own homework'. There is no requirement in NERC CIP for a segregation of duties around compliance work and less security mature organisations may have gaps in their security which are not identified or covered up.
- The cost of compliance to NERC CIP has caused security priority concerns. Previously, there has been a trade-off between meeting the compliance requirements and increasing the organisation's security posture 'being more secure'. Also, the costs of compliance requirements are often not included in the costs that are recoverable by the regulator. This can make the operation of CNI less profitable and thus draws in less investment.

These areas of concern are just a handful of examples. As we continue to progress through this work package to validate models around regulatory structures, more real and theoretical examples will be identified.

Conclusion

In this report we have presented the information/cyber security scenarios of Work Package 2 which have been constructed to cover the entire picture of National Grid's UK Critical National Infrastructure in the current state and the short to medium term future. For the current state, both threat and risk assessments are completed for the different business areas in scope. The future state consists of the future and emerging threats that were identified in numerous internal National Grid workshops and external security roundtable meetings.

This report presents the requirements for Work Package 2 which focus on understanding and assessing the information/cyber security regulatory frameworks that are or could apply to Critical National Infrastructure operators. Given that National Grid operates CNI in both regulatory environments this presents an excellent opportunity for the wider Seconomics projects, in collaboration with the other project partners, to assess their efficacy. In particular

- Do the current CNI regulations in the UK and US 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?
- Which regulatory structures, whether risk-based, rules-based or something else, would be better in the current and future states? And can we look at examples elsewhere in the world or in other industries?

These questions form the key requirements of this work package. Together with work packages 4, 5 and 6, by utilising the threats and risk identified in the current and future states we aim to answer these questions above and build policy recommendations based upon those answers. Then through the engagement plan presented in Section 3 we aim to disseminate this information to the government regulators and agencies at the national and supranational level.

6. References

1. D2.2 National Grid Requirements – First Version, FP7 - Seconomics Report. R. Ruprai (NGRID), J. Williams (UNIABDN).
2. HMG Information Assurance Standard No. 1 – Technical Risk Assessment v3.51. CESG – The National Technical Authority for Information Assurance and the Cabinet Office (2009).
3. Standard CIP-001-2a: Sabotage Reporting. North American Electric Reliability Corporation (2011).
4. Standard CIP-002-3(a): Cyber Security – Critical Cyber Asset Identification. North American Electric Reliability Corporation (2012).
5. Standard CIP-002-4a Cyber Security - Critical Cyber Asset Identification. North American Electric Reliability Corporation (2012).
6. Standard CIP-003-3: Cyber Security – Security Management Controls. North American Electric Reliability Corporation (2009).
7. Standard CIP-004-3: Cyber Security – Personnel & Training. North American Electric Reliability Corporation (2012).
8. Standard CIP-005-3a: Cyber Security – Electronic Security Perimeter(s) . North American Electric Reliability Corporation (2010).
9. Standard CIP-006-3c/d: Cyber Security – Physical Security of Critical Cyber Assets. North American Electric Reliability Corporation (2010).
10. Standard CIP-007-3: Cyber Security – Systems Security Management. North American Electric Reliability Corporation (2009).
11. Standard CIP-008-3: Cyber Security – Incident Reporting and Response Planning. North American Electric Reliability Corporation (2009).
12. Standard CIP-009-3: Cyber Security – Recovery Plans for Critical Cyber Assets. North American Electric Reliability Corporation (2009).
13. Electricity Act 1989, Great Britain. Her Majesty's Government UK Legislation (1989)
14. Electricity Transmission Licence: Standard Conditions. Her Majesty's Government UK Legislation (2012)
15. Federal Energy Regulatory Commission website https://www.ferc.gov/
16. North American Electricity Reliability Corporation website http://www.nerc.com/
17. Other National Grid internal sources and documents

Appendix 1

In this Appendix we present tables of Business Impact Levels (BILs) compiled from a number of BIL tables in HMG IS1[8].

Table 9 - 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

[8] 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-term 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 10 - 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[9] referenced within this document.

Table 11 gives the metrics for Threat Actor Capability which ranges from 1 (Very Little) to 5 (Formidable).

Table 11 - Threat Actor Capability

Capability	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

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

Table 12 gives the metrics for Threat Actor Motivation which ranges from 1 (Very Low - Indifferent) to 5 (Very High - Focused). In HMG IS1 there is 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. There are 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 12 - 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 13 presents a matrix of the product of Capability and Motivation which leads to Threat Level.

Table 13 - 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 14 presents a matrix of the product of Business Impact Levels and Threat Levels which gives the Risk Level.

Table 14 - 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

Table 15 shows the activities that we undertook to identify and validate the information presented in this deliverable.

Table 15 – Validation activities for WP2 deliverables

Date	Activity	Detail & Topic
13/04/2012	ENTSO-E Brussels	Discussion on specific security issues around the Electricity Highway
25/04/2012	STEG	GB Smart Metering Programme security forum, engagement with CPNI and DECC
30/04/2012	DR&S	Seconomics introduction to internal DR&S team
03/05/2012	Workshop with external strategy consultant	Initial discussion of key stakeholders nationally and supranationally
10/05/2012	NG site visit	Visit to London Power Tunnels – significant investment in CNI
17-19/05/2012	WP2 workshop meeting	UNITN, UNIABDN workshop on stakeholders, current and future threats
22/05/2012	STEG	GB Smart Metering Programme security forum, engagement with CPNI and DECC
29/05/2012	Threat assessment discussion with Head of I&TM	Call to discuss different sources of threats
09-11/06/2012	NG Leadership meeting	Introduction to Seconomics to NG Leadership Brief discussion of WP2 key requirements
18-20/06/2012	DR&S team meeting	Face-to-face team meeting of all global DR&S staff Discussion of CNI threats and maturity with CNI network team and other staff Discussion with CISO on requirements of WP2
27/06/2012	ENISA Smart Metering Grid	Introduction to Seconomics and key requirements of WP2 to international European organisations including: ENISA, TSO's and vendors
02-04/07/2012	WP2 and 6 meeting	Collaboration between WP2 and WP6. Discussion of requirements and regulatory systems, incentives and economic models
05/07/2012	Workshop with external strategy consultant	Mapping out of WP2 key stakeholders
09-13/07/2012	Meeting with NG CISO	Summary and review of D2.2.
16-19/07/2012	CNI networks	Understanding how CNI networks operates and are

	meeting in the US	organised in the US Discussion of NERC CIP requirements and implications on CNI network teams
30/07/2012	Meeting with transmission managers UK	Understanding CNI information security business impacts assessment on transmission
23/08/2012	Meeting with TNCEIP team	Identification and transfer of threat sources
06/09/2012	DR&S threats session	Workshop discussing current, changeable and future threats to CNI with NG CISO and DR&S Heads
14/09/2012	STEG	GB Smart Metering Programme security forum, engagement with CPNI and DECC
11/10/2012	STEG	GB Smart Metering Programme security forum, engagement with CPNI and DECC
16-18/10/2012	Meeting with UNIABDN	Discussion of WP2 key requirements and modelling options for WP6
19/10/2012	Workshop with external strategy consultant	Seconomics engagement plan discussions following from stakeholder map in D2.2
25/10/2012	STEG	GB Smart Metering Programme security forum, engagement with CPNI and DECC
06-09/11/2012	Seconomics General Assembly Madrid	Dissemination of WP2 with other project partners
14/11/2012	ENTSO-E CSP WG	Dissemination of Seconomics' aims, objectives and progress Request for surveying other TSO's regulatory structures
15/11/2012	STEG	GB Smart Metering Programme security forum, engagement with CPNI and DECC
16/11/2012	Workshop with NG Security consultants	Assessment and consolidation of current threats and risks using HMG IS1 framework
30/11/2012	Electricity Control Centre Visit	Training session and site visit to further understand electricity management and balancing
06/12/2012	Workshop with NG Security consultants	Assessment and consolidation of current threats and risks for each business object using HMG IS1
10-14/12/2012	DR&S Internal review	Scientific review of threats and risks assessment Technical review of electricity transmission background
10-14/12/2012	European Engagement plan review	Review of Stakeholder map and engagement plan
13/12/2012	STEG	GB Smart Metering Programme security forum, engagement with CPNI and DECC
17-19/12/2012	NG CISO review	Review of entire Deliverable D2.3 focussing on security scenarios and regulation sections

02-04/01/2013	Scientific review	Seconomics scientific review
14-16/01/2013	NG CISO review	Final Review of Deliverable D2.3
18/01/2013	SSRC meeting	Security scrutiny meeting number two to verify the release of deliverables D1.3, D2.3 and D3.3

Appendix 4

CNI Security Scenarios – Current State Impact, Threat and Risk Assessments for:

- Interconnectors
- Electricity Management System and its data links with generators, distributors and interconnectors
- Corporate Network and IT Infrastructure supporting Electricity Transmission,

have been included as a separate annex. Due to the sensitive information/cyber security nature of the impact, threat and risk assessments, they can only be shared upon request and following an internal assessment by National Grid.