AEA

Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector

risksolutions
leave nothing to chance

ESR Technology
Engineering, Safety & Risk

DIALOGIK

Final Report to European Commission
Directorate-General Justice, Freedom and Security

Restricted Commercial

4th September 2009

Title	**Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector**
Customer	**European Commission** Directorate-General Justice, Freedom and Security
Customer reference	JLS/2007/D1/026
Confidentiality, copyright and reproduction	Copyright European Commission
File reference	ED05761
Reference number	ED05761101

AEA
Gemini Building
Didcot
Oxfordshire
OX11 0QJ

t: 0870 190 8435
f: 0870 190 6318

AEA is a business name of AEA Technology plc

AEA is certificated to ISO9001 and ISO14001

Author	Name	Jonathan Perks, Jonathan Hyde, Angela Falconer
Approved by	Name	Peter Sage
	Signature	
	Date	4th September 2009

Executive summary

This is the Final Report for the Directorate General Justice Freedom and Security (DG JFS) project: Study on Risk Governance of European Critical Infrastructures in the ICT and energy sector.

The primary goal of this project was to propose a Risk Governance Framework for European CIs in the interface between the ICT and energy sector, based on the analysis of actors, regulatory, market and technical factors, decision processes, problem framing, development of risk scenarios and application to them of a Risk Governance Framework. In addition we were asked to provide suggestions on how to implement the results of this study.

A Risk Governance Framework based on the International Risk Governance Council (IRGC) model has been developed. This report describes how the framework was developed, including significant involvement of stakeholders, and describes the framework. The framework is presented, in an Annex, as a stand-alone format that can be used by stakeholders when they are carrying out the risk governance process. Finally the report draws out conclusions and makes recommendations for the implementation of the framework.

Table of contents

1 Introduction

1.1 The Project

The security and economy of the European Union as well as the well-being of its citizens depends on certain infrastructures and the services they provide. The destruction or disruption of infrastructures providing key services could entail the loss of lives, the loss of property, a collapse of public confidence and moral in the EU. Any such disruptions or manipulations of critical infrastructure should, to the extent possible, be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the Member States, their citizens and the European Union. The recent terrorist attacks in Madrid (2004) and London (2005) as well as the Estonian cyber attacks (2007) and the German Blackouts (2006) have highlighted the potential vulnerability of European infrastructure both from terrorism as well as other operational failures. Furthermore the current banking crisis has highlighted the need for appropriate national and regional government organisations to be reassured that organisations operating and regulating key national and regional infrastructures have adequate risk governance processes in place, not only to protect their own business continuity, but also to protect the wider communities.

As part of its response, the European Commission has introduced the European Programme for Critical Infrastructure Protection (EPCIP). As well as general measures, the programme calls for sector-specific assessments.

The European Commission defines a 'Critical Infrastructure' as "an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of a failure to maintain those functions". In addition "'European Critical Infrastructure', or 'ECI' means critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States"[1].

Without a European approach to understanding the decision making process for dealing with risks to European Critical Infrastructures, quantifying the risk of such disruptions is difficult. Private decision-makers will have neither adequate information nor adequate motivation to undertake investments that are more than justifiable from the standpoint of the system as a whole.

In particular EC is concerned about the vulnerability of critical infrastructures in the ICT and Energy sector in Europe and ensuring the security of energy supplies. This applies to all critical infrastructures in Europe regardless of whether they can be considered as having EU or national importance. The scope of the study is therefore to focus on the decision making process for dealing with ECI risk governance between the ICT and energy sector.

This project was commissioned by the European Commission's Directorate of Justice, Freedom and Security (DG JLS) to develop a Risk Governance Framework for ECIs in the interface between the ICT and energy sector, based on the analysis of actors, regulatory, market and technical factors, decision processes, problem framing, development of risk scenarios and application to them of a Risk Governance Framework.

The project began with an assessment of the existing approaches to managing risks in the energy / ICT sector, carried out analysis of the requirements of a Risk Governance Framework by seeking the opinions of relevant stakeholders, before finally developing a Risk

[1] COUNCIL DIRECTIVE 2008/114/EC on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection, Brussels, 08.12.2008, COM(2006) 787 final

Governance Framework based on the model developed by the International Risk Governance Council and recommending how it is used.

This is the final report of the project which describes the approach, the Risk Governance Framework and recommendations for its implementation.

1.2 Project Goals

The primary goal of this project was to:

- Propose a Risk Governance Framework for ECIs in the interface between the ICT and energy sector, based on the analysis of actors, regulatory, market and technical factors, decision processes, problem framing, development of risk scenarios and application to them of a Risk Governance Framework.

- Provide suggestions on how to implement the results of this study (e.g., to prepare a pilot project, awareness raising campaign, workshops, seminars, conferences, etc).

1.3 Report Structure

1. **Introduction:** The present chapter introduces the report and the aims and structure of the project.
2. **Context:** Provides context for the analysis, including a review of the critical Infrastructure Protection, the European Energy Supply System and the Energy-ICT interfaces.
3. **Methodology:** describes how we carried out this project.
4. **Analysis:** describes our key findings which were used to develop the Risk Governance Framework.
5. **Risk Governance Framework:** sets out the proposed Risk Governance Framework.
6. **Recommendations and Conclusions:** lists the main conclusions and recommendations derived from the project.
7. **Glossary:** provides a concise explanation of the terms used in the report.

Annexes

The annexes provide further information from the key activities of the project:

Annex 1: **Literature Review:** provides a summary of the literature publicly available.

Annex 2: **Stakeholder Workshop 1:** provides the notes of the first Stakeholder Workshop held in March 2009.

Annex 3: **Risk Governance Questionnaire:** is the questionnaire used to obtain information from stakeholders.

Annex 4: **Stakeholder Workshop 2:** provides the notes of the second Stakeholder Workshop held in June 2009.

Annex 5: **Risk Governance Framework with Templates:** is a stand-alone document containing the Risk Governance Framework with templates which can be completed as the tool is used.

Annex 6: **Case Study Application for the Risk Governance Framework:** provides a worked example using the Risk Governance Framework.

Annex 7: **ICT / Energy System Interfaces:** Identifies the main ICT /Energy interfaces.

Annex 8: **Example Defences:** Suggests some of the defences which may be used to prevent / mitigate against failures at these interfaces.

Annex 9: **Policy Brief:** contains a stand-alone Policy brief summarising the project and providing the key conclusions and recommendations.

The Policy Brief is produced as a separate document for wider circulation as considered appropriate by DG JLS.

1.4 Project Team

The project was carried out by AEA in partnership with Risk Solutions, DIALOGIK and ESR Technology.

AEA is a leading international energy and environmental company specialising in consultancy, policy support and programme management for policy implementation. AEA has an extensive track record with the European Commission, including a recent high-profile project under EPCIP relating to critical energy infrastructures. We bring a clear understanding of the Commission's requirements, as well as expertise in project management and stakeholder engagement, at EU level in the energy sector.

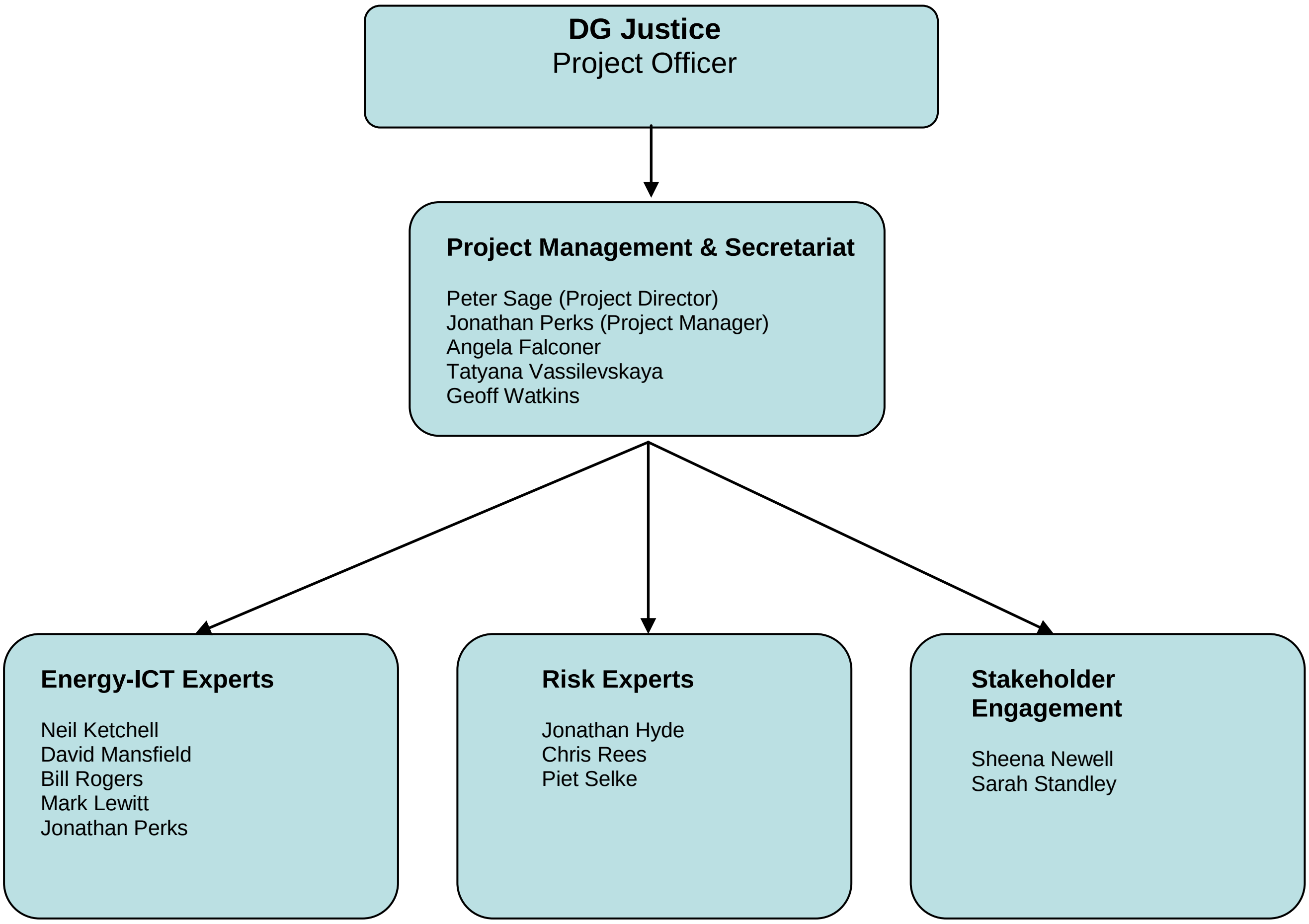
Risk Solutions origins stem from developing and applying state of the art risk management methods in the nuclear energy and chemical process industries. Risks Solutions is a team of strategic thinkers, with a strong analytical grounding across several business sectors, including rail and road transport, central government, and energy, with proven project management capabilities, working closely with both clients and key project stakeholders. They provide controls assurance and risk management consultancy services to a wide range of clients.

DIALOGIK brings special competence and experience into the proposed project with regard to the conceptual-analytical design of risk governance issues for security issues. DIALOGIK has acted as the coordinator of the PrecauPri-project which developed a policy framework for precautionary and participatory risk regulation in Europe (which was tested using new organic chemicals as a case study) and as coordinator of that subproject of the Safe Foods project which was entrusted with the investigation of institutional challenges and solutions to the implementation of a food safety governance system which is more inclusive and integrative in these terms: by building on both natural scientific expertise and social scientific expertise as well as systematic and experiential knowledge, and by involving the four major actors in risk decision making, i.e. political, business, scientific and civil society players, in the process of framing the problem, generating options, evaluating options, and coming to a joint conclusion.

ESR Technology (ESRT) was formerly the Engineering, Safety and Risk business of AEA Technology. ESRT incorporates all the expertise, staff and facilities from that business and thus brings a heritage of more than 40 years experience of the application of engineering excellence to demanding projects. ESRT continues to specialise in the provision of independent technical expertise, products and services to help their Customers: Ensure Asset Integrity, Improve Machine Reliability, Manage Safety & Risk, and Transfer Best Practice. ESRT's highly skilled, world-class consultancy teams have in-depth experience of working with Customers across many sectors, including: Oil & Gas; Rail; Utilities; Aviation; Space and Defence.

Figure 1.1 shows the key people who worked on the project. Several of the core team members, including Peter Sage, Jonathan Perks, Angela Falconer, Neil Ketchell, David Mansfield and Chris Rees previously worked on the project "Definition of Critical Infrastructures at EU level in the Energy Sector" for EC DG TREN (Energy and Transport).

Figure 1.1 Project Team



DG Justice
Project Officer

Project Management & Secretariat

Peter Sage (Project Director)
Jonathan Perks (Project Manager)
Angela Falconer
Tatyana Vassilevskaya
Geoff Watkins

Energy-ICT Experts

Neil Ketchell
David Mansfield
Bill Rogers
Mark Lewitt
Jonathan Perks

Risk Experts

Jonathan Hyde
Chris Rees
Piet Selke

Stakeholder Engagement

Sheena Newell
Sarah Standley

2 Context

This section of the report provides an overview of the rationale for developing a Risk Governance Framework for the energy-ICT sector. It does so by firstly introducing the challenges faced in the energy sector with regard to security of ICT systems and secondly by reviewing EU activities to date to overcome those challenges. The resultant need for an overarching framework of risk governance to ensure common standards of risk management are applied with respect to EU critical infrastructures is then introduced.

2.1 The European Energy Supply System

2.1.1 Dependency and Interconnectedness

As stated in the Green Paper of 2006[2], the EU is highly dependent on continued access to sustainable, competitive and secure sources of energy. Any disruption to energy supply can have considerable impacts on the health, safety, security and economic wellbeing of European citizens.

It is clear that of all the systems the failure of electrical supply system has the most rapid and wide-ranging impact. For example, without electricity all forms of transport are quickly affected as control systems (traffic lights, rail signals) and communications systems cease to operate. Water and sewage systems stop when pumps and controls are not operating and financial systems cease to function without modern communications equipment (as when the Colombian stock exchange ceased trading during a nationwide black-out in April 2007).

This is further illustrated by events in Germany in 2006. Here the electrical black-out halted the rail system as not only were electric trains without power but signalling and communication systems also rely on power for operation. The event also demonstrates the interdependent and interconnected nature of the EU electricity grid whereby a fault in one country affected 15 million households across Europe including Italy, Spain and Austria.

Several major challenges affect the European energy supply system at present. These include:

- Increasing demand. There are almost a quarter of a billion electricity customers in Europe at present, concentrated mostly in Germany, the UK, France and Italy. Total electricity consumption in the EU-27 amounted to 2843 TWh in 2007[3]. EU PRIMES analysis assumes that annual consumption will grow by 1.9 % on average until 2010[4], particularly in southern Europe and central Eastern Europe[5]. Final electricity demand in the EU is expected to increase by 8-28%[6] from 2005 to 2030 (depending on price assumptions), requiring additional generation capacities. The EU's natural gas consumption is expected to increase from 445 million tonnes of oil equivalents (Mtoe) in 2005 to 516 Mtoe in 2030. EU-27 oil demand is predicted to increase from 665 Mtoe in 2005 to 708 Mtoe in 2030 under the PRIMES 2007 Baseline scenario[7].

- The development of the EU internal energy markets in electricity and gas. Many national energy markets remain heavily protected and dominated by monopolies, resulting in high energy prices and lack of investment in infrastructure.

- The management of an increasingly interconnected, complex EU energy system.

[2] Green Paper COM/2006/0105 - A European Strategy for Sustainable, Competitive and Secure Energy

[3] Eurostat, (2009), http://epp.eurostat.ec.europa.eu/portal/page/portal/energy/data/database,[Accessed 12 August 2009]

[4] European Energy And Transport Trends To 2030 — Update 2007, http://www.energy.eu/publications/KOAC07001ENC_002.pdf

[5] Vattenfall., 2005. *Annual Report 2005*. [Internet]. Available from: www3.vattenfall.com/annual_report_2005/filter.asp?filename=page_011.html [Accessed 13 February 2007]

[6] DG TREN, (2008), Europe's energy position past and future

[7] European Energy And Transport Trends To 2030 — Update 2007, http://www.energy.eu/publications/KOAC07001ENC_002.pdf

- Ageing energy infrastructures requiring substantive investment. One implication of this is that the older equipment may have used old style electromechanical or basic 'stand alone' PLC logic controllers which are less prone to cyber attack, whereas any replacement equipment will almost certainly use modern digital control equipment linked to DCS (Digital Control Systems) and SCADA systems, with all the characteristics this brings. There is an urgent need for investment. In Europe alone, to meet expected energy demand and to replace ageing infrastructure, investments of around one trillion euros will be needed over the next 20 years. [8]

- The expansion of the EU energy market into the EU neighbourhood via the Energy Community.

- Environmental concerns (including climate change, radioactive waste disposal and other pollution).

- Geopolitical and terrorism risk.

- Management of intermittent distributed generation on the electricity grid.

- Import dependence. Reserves are concentrated in a few countries. Today, roughly half of the EU's gas consumption comes from only three countries (Russia, Norway, Algeria). All 27 EU Member States, except Denmark, depend to some extent on imports from neighbouring and non-EU states to meet energy demand. Member States with highest import dependence (percentage of gross consumption fed by net imports) in 2008 are Cyprus, Malta (both have an energy dependence rate of 100%), Luxembourg (99%) and Ireland (91%). In total, 54%[9] of the EU's energy demand is met by imports and this is predicted to increase to 70% in the next 20 to 30 years.[10] Gas import dependence is predicted to rise from 54% in 2005 to 84% under a business as usual scenario, with the most likely source being the Middle East. Oil import dependence is expected to increase from the current level of 80% to above 90% in 2030[11].

- Oil and gas prices are rising and have almost doubled in the EU over the past two years, with electricity prices following. This is difficult for consumers. Increased prices are driven by increasing global demand for fossil fuels, stretched supply chains and increasing dependence on imports, high prices for oil and gas.

These challenges summarise the context in which physical energy infrastructures are developed and managed. Within the EU energy supply system, transfers of energy are largely conducted through shared infrastructures, except in the case of 'energy peninsulas' such as the UK and the Nordic states. Gas and oil are distributed through networks of major pipelines from outside the EU. These networks are illustrated in Figure 2-1 and
Figure 2-2.

The Union for the Co-ordination of Transmission of Electricity (UCTE) (now the European Network of Transmission System Operators for Electricity (ENTSO-E)) co-ordinates a complex synchronously interconnected electricity system linking 24 countries across mainland Europe. National or operators' systems are connected and run collectively, at the same frequency. This provides considerable fall back in the event of a system disturbance in one country but conversely opens the European system up to a domino effect whereby

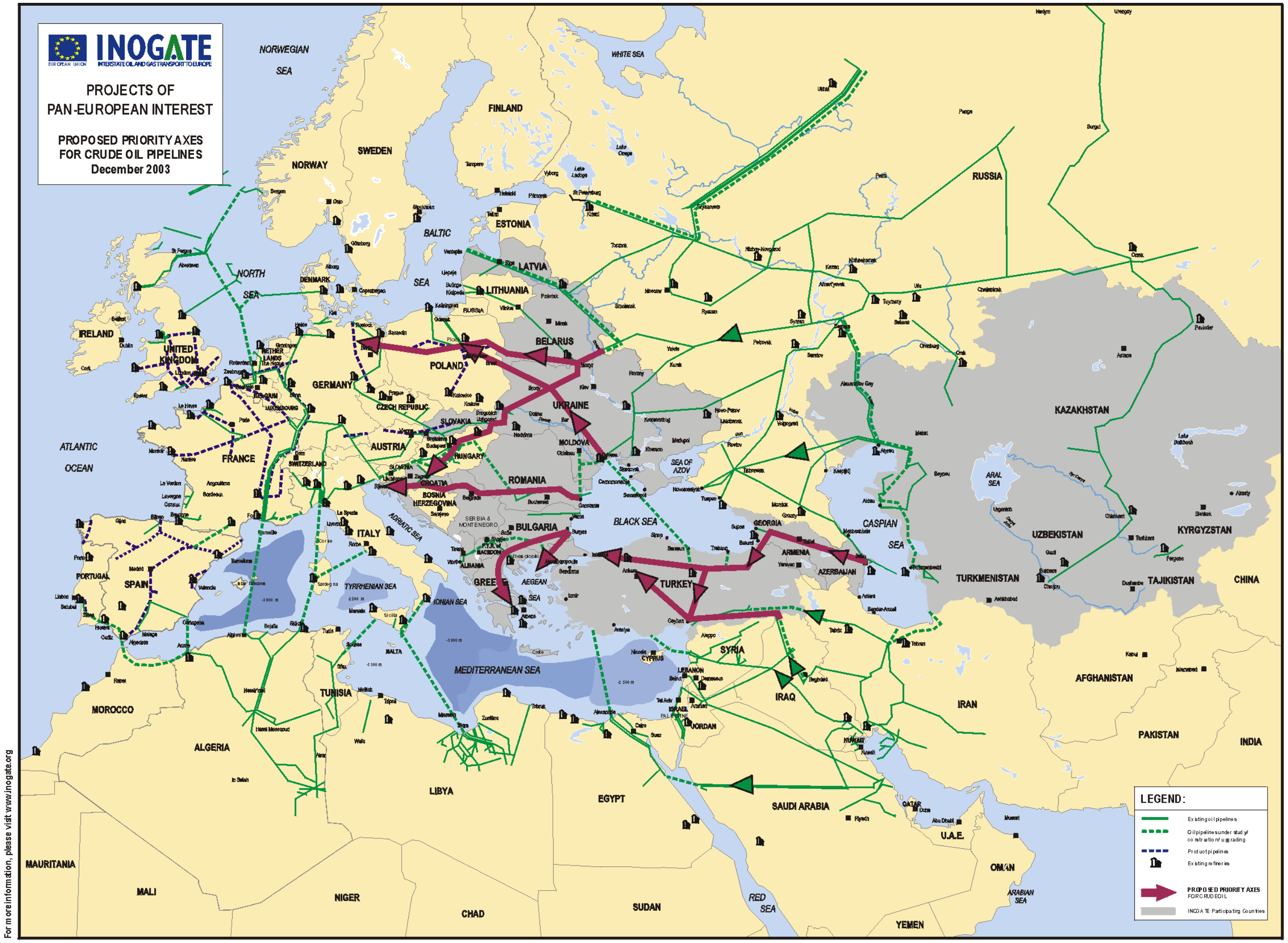
[8] Green Paper COM/2006/0105 - A European Strategy for Sustainable, Competitive and Secure Energy
[9] Europe's energy portal, www.energy.eu [Accvessed July 2009]
[10] Eurostat., 2006. "*Energy in the EU: First Estimates*". Eurostat News Release126/2006. [Internet]. Available from: epp.eurostat.ec.europa.eu/pls/portal/docs/PAGE/PGP_PRD_CAT_PREREL/PGE_CAT_PREREL_YEAR_2006/PGE_CAT_PREREL_YEAR_2006_MONTH_09/8-21092006-EN-AP1.PDF [Accessed 13 February 2007]
[11] European Parliament ITRE Committee., 2006. *The potential and reserves of various energy sources, technologies furthering self-reliance and the impact of policy decisions*. [Internet]. www.europarl.europa.eu/comparl/itre/pe375854_en.pdf [Accessed June 2006]

disturbance has the potential to migrate into neighbouring countries with a high level of connection and dependence[12].

In addition to energy distribution networks, the EU energy system is dependent on a wealth of individual infrastructures to extract, generate, process, store and control oil, gas and electricity. Many of these networks and infrastructures are critical to the continued supply of energy to meet the needs of the EU.

[12] UCTE., 2007. *Operation of the System*. [Internet]. (Updated 5 Jan 2004).
Available from: www.ucte.org/ourworld/Control-Blocks/e_default.asp [Accessed 13 February 2007]

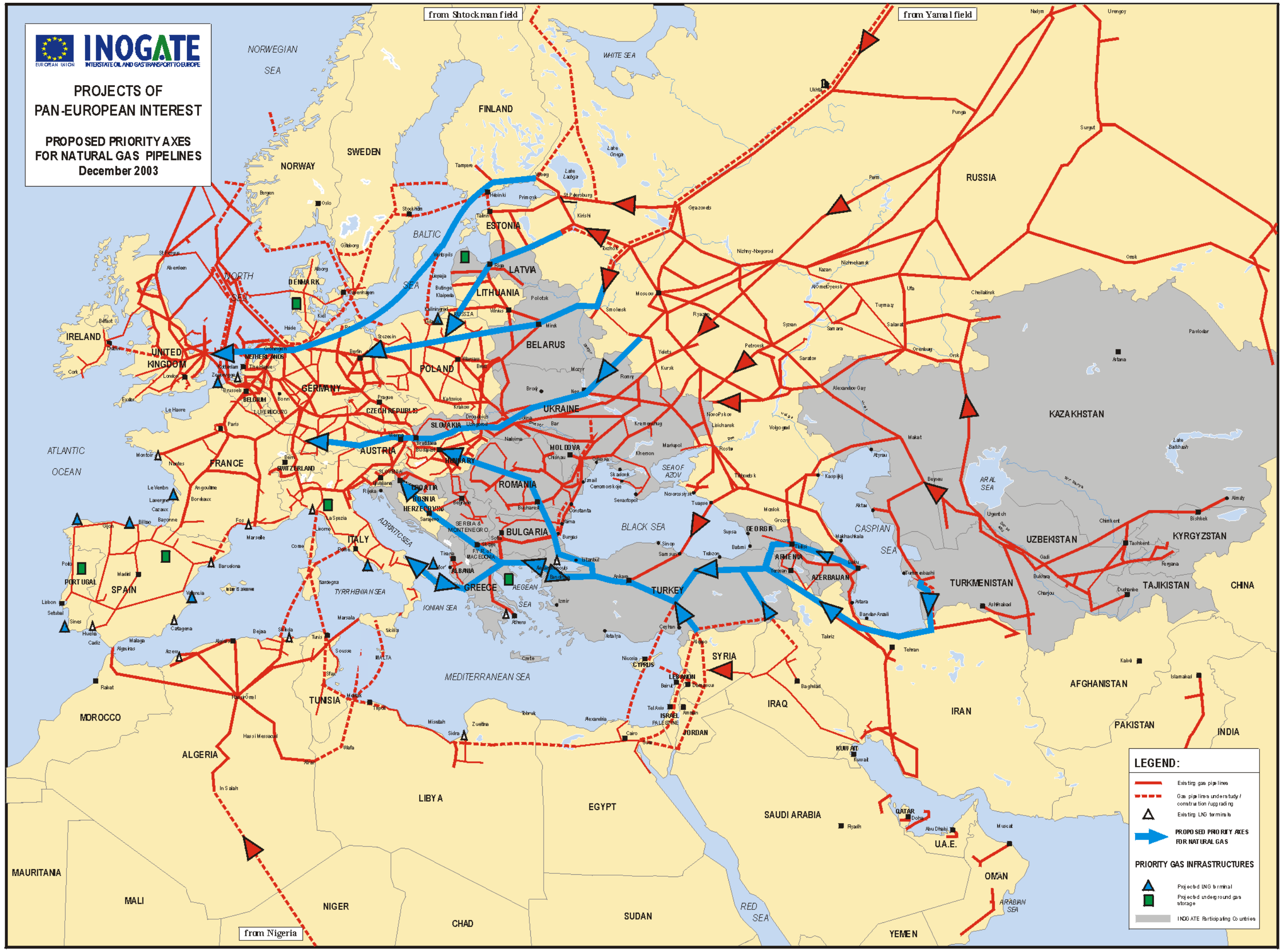
Figure 2-1: European oil pipeline network



This publication is produced with the assistance of the European Union. The contents of this publication are the sole responsibility of the contractor, EIR / Hill / G&Fint, and can in no way be taken to reflect the views of the European Union.

Source: Inogate

Figure 2-2: European gas pipeline network



For more information, please visit www.inogate.org

This publication is produced with the assistance of the European Union. The contents of this publication are the sole responsibility of the contractor, EIR / Hill / G&F int, and can in no way be taken to reflect the views of the European Union.

Source: Inogate

2.1.2 Critical Energy Infrastructures

The EU defines a critical infrastructure as “an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions”[13].

The project *Definition of Critical infrastructures at EU level in the energy sector*[14] concluded that Critical infrastructures tend to be nodes located on or near key transmission lines. Therefore, the most EU-critical infrastructures in each domain tend to be:

- Electricity *Substations and interconnectors*
- Gas *Compressor stations on major pipelines*
- Oil *Ports and major pipelines*

Criticality at the most basic level is affected by the intrinsic nature of the energy domain in question, dictating important factors such as ease of storage and flexibility.

Electricity is the most EU critical energy domain. This is because the system has to be kept in balance in real time; because disruptions can spread in seconds; and because the consequences of a blackout are often severe. Substations and interconnectors are often more critical than power stations.

The most EU-critical parts of the gas system are compressor stations on major pipelines. Several pipelines are also important but criticality is reduced by relatively quick repair times (in comparison to compressor stations). Unlike electricity and oil, dependence on gas is highly country specific.

Oil infrastructures tend to be less EU-critical than electricity and gas infrastructures. Oil remains a critical fuel for transportation in every Member State. However, the market is global, supply is flexible and storage levels are significant. Under Community law, each Member State is required to store over 90 days of domestic demand. Oil infrastructures critical to EU supplies tend to be located beyond the EU.

There have been a number of significant energy disruptions caused by operational faults in recent years. In the electricity sector, these have often been made more significant by escalation. The evidence suggests that EU energy systems are vulnerable to disruption, especially a deliberate and planned attack.

The project concluded that the EU energy system is configured on a commercial – not security – basis. This applies to the physical infrastructure and virtual architecture as well as processes and procedures.

In addition, the potential for infrastructure disruption is typically seen from the perspective of technical failure – as opposed to a deliberate attack. This is reflected in, for example, spares strategies and emergency response management. It is possible for single point failures to propagate if the initial system conditions are unusual. Especially in the electricity sector, this can escalate to cause a significant disruption. A multiple attack by terrorists could result in several disruptions at different sites. In the electricity domain, an attack on several transmission lines could cause instability at the system level.

[13] Directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection (2008/114/EC).

[14] AEA (2007). The remit of this project was to evaluate the criticality and vulnerability of the existing energy infrastructure, with a view to informing the future identification and designation of EU critical energy infrastructures.

A Critical Infrastructure Protection (CIP) approach requires us to revisit these norms in order to consider the implications of a deliberate and planned attack on energy systems. In many cases, the solutions are additional to those implied by a traditional approach, but in some cases there is a potential conflict.

It is therefore equally important to create resilient energy systems as it is to protect specific critical infrastructures. This implies an emphasis on issues such as:

- Planning standards.
- Communications and data sharing between TSOs.
- Emergency planning.
- Training – with a transnational dimension.
- Coordination and leadership.

As much critical infrastructure is owned or controlled by national publicly owned or privately owned organisations there is an increasing requirement to understand the business and operational sides of these sectors in order to ensure that there are appropriate regulations and mechanisms in place to ensure security of supply across Europe, consistent with the principles of subsidiarity.

2.1.3 The Energy-ICT Interface

Both ICT and Energy were identified as Critical Infrastructure sectors by the European Programme for Critical Infrastructure Protection (see section 2.2). With modern widespread and interconnected ICT systems there is a risk of cascading effects causing more and more systems to fail from a single initial failure. There are crucial links between physical and virtual architectures so that when one fails the other is likely to be compromised unless appropriate protection is in place.

In the energy sector, ICT is crucial for:

- Energy monitoring, distribution and control of systems (including crucially fault communication), and trading in energy and fuels. Ensuring every day operability and system resilience. Including SCADA and Network Management Systems. This also includes the DCS and SCADA systems associated with oil & gas production facilities onshore and offshore, LNG/gas terminals and refineries, crude oil/ products and gas/LNG storage depots, etc.
- Operational, response and safety communications: Crucial in the event of a disruption.
- Automatic Protection Systems: These systems detect faults and disconnect services quickly to ensure stability of systems. Examples include automated system control via private networks or the internet.
- Data: Data is fundamental to correct operation of ICT systems both under normal conditions and also critically under abnormal system conditions; current and forecasted demand and supply of services, planning information, plant status information. Data corruption, or lack of access to required data can disrupt the balance of a system; implemented control measures and recovery may be delayed.

SCADA (Supervisory Control and Data Acquisition) systems are a key element in the safe and secure operation of both installations and extended infrastructures. SCADA systems collect, display and store information from remotely located data collection transducers and sensors to support the control of equipment, devices and automated functions. They form part of the Process Control System that is used to manage in real time, for example, the transmission and distribution of electricity and pressure and flow of gas pipelines.

The advantages SCADA brings to business competitiveness such as the ability to control multiple processes, reduced travel on-site and pro-active management have led to widespread adoption in complex critical infrastructures. However, the benefits of a single point of control and the extensive use of networking also mean that if they were to be subjected to malicious attack they could cause far greater damage and widespread disruption.

Four key threats to SCADA are:

- Malware – for example worms, viruses, Trojans and spyware.
- Insider attack – either accidental or, for example from a disgruntled employee.
- Hacker – an independent external attacker who may be breaking on to the system because of the challenge it presents.
- Cyber Terrorist - since they can cause widespread damage to a large proportion of the population.

When many SCADA systems were initially installed, the threat posed by the current security environment and the increasing reliance on common software, operating systems, public telecommunications systems and the Internet, were not well realised. Furthermore it has been difficult for operators to assess the vulnerability of their, often complex, operational control systems and verify the performance of proposed security upgrades prior to installation.

ICT systems can malfunction for a number of reasons – such as human error; hardware and software failure; and malicious activity. Malicious activity can be targeted to a sector or organisation, or have an effect on the sector via untargeted threats such as viruses.

The project *Definition of Critical infrastructures at EU level in the energy sector*[15] found that:

- The number of cyber attacks has significantly increased in the past decade.
- Increasingly these attacks arise from external sources.
- There is considerable variation in the awareness and preparedness of Member States to the threat.
- A cyber attack could have a very serious impact on the electricity and gas systems, in particular.

2.2 EU Activities to date in the field of Critical Infrastructure Protection and Cyber Security

This section of the report reviews EU policy developments on critical infrastructure protection, particularly during the past five years. The section then focuses on EU policy in the field of cyber security.

2.2.1 Critical Infrastructure Protection

The European Dependability Initiative (EDI) was implemented in 1998-1999, representing a major research effort in the European Union to address the issues of the critical infrastructure protection and survivability efforts in the United States, and included plans for joint EU-US collaboration in this sphere [Carnegie Mellon University 2001]. The EDI recognised an ever-growing dependence of the modern information society upon software-based control systems, communication applications and services. It also acknowledged that the extensively deployed nature of new technologies was giving rise to new types of problems and challenges for dependability technologies. [EDI 1998]

[15] AEA (2007). The remit of this project was to evaluate the criticality and vulnerability of the existing energy infrastructure, with a view to informing the future identification and designation of EU critical energy infrastructures.

Following the EDI, the Dependability Development Support Initiative (DDSI) was run between June 2001 and November 2002. DDSI acknowledged the increasing dependence of a wide set of European infrastructures, including energy generation and distribution, on networked information systems which results in the vulnerability of critical businesses and social processes to accidental or malicious failures of IT systems and networks. It also recognised the necessity of developing comprehensive policy initiatives at the European level to help protect citizens, support business and secure critical infrastructures [DDSI 2007]. DDSI [2002] notes that the critical infrastructure protection remains a Member State responsibility. Nonetheless, growing competencies of European institutions in relation to European security and foreign policy and the increased European policy focus on large-scale terrorist attacks are leading to a recognition that enhanced European-wide cooperation is required if risks to interdependent infrastructure are to be managed. [DDSI 2002]

2.2.2 European Programme for Critical Infrastructure Protection

The European Commission initiated a programme on critical infrastructure protection (EPCIP) in 2004 with the publication of the Communication entitled "Critical Infrastructure Protection in the Fight against Terrorism". Following work to define the programme, a Green Paper on a European Programme for Critical Infrastructure Protection (COM (2005) 576 final) was released in 2005 and further elaborated in 2006 in the Communication on a European Programme for Critical Infrastructure Protection. The stated objective of EPCIP is to improve the protection of critical infrastructure in the European Union (EU). This objective is to be achieved by establishing:

- A procedure for identifying and designating European critical infrastructure and a common approach to assessing the need to improve the protection of such infrastructure.

- Measures designed to facilitate the implementation of EPCIP, including an EPCIP action plan, the Critical Infrastructure Warning Information Network (CIWIN), the setting up of Critical Infrastructure Protection (CIP) expert groups at EU level, CIP information sharing processes, and the identification and analysis of interdependencies.

- Support for Member States regarding National Critical Infrastructures (NCIs) that may optionally be used by a particular Member State.

- Contingency planning.

- An external dimension.

- Accompanying financial measures, and in particular the Specific EU Programme on "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" for the period 2007-13, which funds opportunities for CIP related measures. [DG Justice, 2009][16].

2.2.3 Directive on the Identification and Designation of European Critical Infrastructure and the assessment of the need to improve their protection

In December 2008, the Council of the European Union adopted the Directive on the identification and designation of ECI and the assessment of the need to improve their protection[17].

The Directive establishes a common procedure for the identification and designation of ECIs and introduces a common approach to the assessment of the needs to improve the protection of ECIs. This assessment will help prepare specific protection measures in the individual sectors.

[16] http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm
[17] 2008/114/EC

- *Casualties* criterion, which is assessed in terms of the potential number of fatalities or injuries;
- *Economic effects* criterion, which is assessed in terms of the significance of economic loss and/or degradation of products or services; including potential environmental effects;
- *Public effects* criterion, which is assessed in terms of the impact on public confidence, physical suffering and disruption of daily life, including the loss of essential services.

The evaluation of security requirements for such infrastructure should be done under a common minimum approach. Protection of the European CIP should build on bilateral schemes for cooperation between Member States in the field of critical infrastructure protection, which constitute an established and efficient means of dealing with transboundary critical infrastructure. [Council of the European Union 2008]

As such, under the Directive, every Member State is required to assess whether each designated ECI located on its territory possesses an Operator Security Plan (OSP) or has in place equivalent measures addressing the security issues. The Operator Security Plan procedure identifies the critical infrastructure assets of the ECI and indicates that security solutions exist or are being implemented for their protection. Operator Security Plans or equivalent measures comprising an identification of important assets, a risk assessment and the identification, selection and prioritisation of counter-measures and procedures should be in place in all designated European Critical Infrastructure. Where such plans do not exist, each Member State should take the necessary steps to make sure that appropriate measures are put in place. It is up to each Member State to decide on the most appropriate form of action with regard to the establishment of Operator Security Plans.

2.2.4 Critical Infrastructure Warning Information Network

On 27 October 2008, the Commission put forward a proposal for a Council Decision on Critical Infrastructure Warning Information Network (CIWIN). This proposal aims to establish the network that would provide the Member States with a secure information, communication and alert system for exchanging information relating to CIP. The system would facilitate cooperation between Member States, allowing for exchanges on threats and vulnerabilities, as well as on strategies for improving the protection of critical infrastructure. Member States' participation in the Network would remain voluntary. The CIWIN would consist of an electronic forum and a rapid alert system, the first for exchanging information and the latter for alerts on risks and threats. It would be a secure classified system, where access to information is regulated accordingly. The development of the technical aspects of the CIWIN is the responsibility of the Commission. [European Union Law 2008]. A pilot version of the system will be deployed in 2009.

2.2.5 European Cyber Security Policy

In recognition of the importance of ICT systems in general the Council of the European Union Framework Decision 2005/222/JHA of 24 February 2005 attacks on information systems identified four types of activity, which Member States were required to criminalise by 16 March 2007:

- Illegal access to information systems - the intentional access without right to the whole or any part of an information system.
- Illegal system interference - the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data.
- Illegal data interference – the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system.
- Instigation, aiding and abetting and attempt - the instigation of aiding and abetting an offence referred to in the preceding three types of activity.

The European Commission's Communication on the fight against cyber crime (SEC 2007/ 641, 642, Brussels, 22.5.2007) sets out the future approach of the EU-wide combat against cyber crime.

The Communication indicated that the number of cyber crimes is growing and criminal activities are becoming increasingly sophisticated and internationalised, frequently organised by criminal groups. However, the number of European prosecutions on the basis of cross-border law enforcement cooperation do not increase. [European Commission 2007]

To address the threats emanating from cyber crime, the European Commission is launching a general policy initiative to improve European and international level coordination in the fight against cyber crime. The objective of this policy is to strengthen the countermeasures against cyber crime at national, European and international level. Further development of a specific EU policy, in particular, has long been recognised as a priority by the Member States and the Commission.

The focus of the initiative will be on the law enforcement and criminal law dimensions of these countermeasures and the policy itself will complement other EU actions to improve security in cyber space in general. The policy will eventually include the following components:

- Improved operational law enforcement cooperation.
- Better political cooperation and coordination between Member States.
- Political and legal cooperation with third countries.
- Awareness raising, training and research.
- A reinforced dialogue with industry and possible legislative action. [European Commission 2007]

In March 2009, European Commission communicated its intention to protect Europe from cyber-attacks and disruptions (Critical Information Infrastructure Protection - a new initiative in 2009[18]). The Commission called for action to protect critical information infrastructures by making the EU more prepared for and resistant to cyber attacks and disruptions. It was recognised that a low level of preparedness in one country can make others more vulnerable, while a lack of coordination reduces the effectiveness of countermeasures.

In this Communication, the European Network and Information Security Agency (ENISA) is foreseen to support this initiative by fostering a dialogue between all actors and the cooperation necessary at the European level. ENISA is an EU Agency, which assists and facilitates the EU and Member States in their efforts to make networks and information systems more secure [ENISA 2007]. It is a source of expert advice and recommendations for the EU Member States and EU Institutions in the area of Network and Information Security (NIS), including provision of information for best practices and facilitation of the contacts between the EU-institutions, Members States as well as the private business and industry actors. ENISA contributes to securing the smooth functioning of the European digital economy and the information society. [ENISA 2008a]

2.3 The Rationale for Developing a Programme of Risk Governance for the ICT-Energy Sector

The operation of EU energy systems is dependent on ICT systems for day-to-day generation, distribution and supply processes and emergency response in the event of disruption. Protecting critical ICT-energy infrastructures requires an understanding of all the vulnerabilities of all the elements that have a bearing on the supply chain reliability. In many cases, dependencies and vulnerabilities cross Member State boundaries. Significant progress has been made to identify dependencies, vulnerabilities and protection measures in both the energy and ICT sectors in the EU through the establishment of operational security standards, research programmes and knowledge sharing networks.

However an overarching governance structure to manage the process of identifying and managing is arguably missing. Effective protection is dependent on communication, coordination, and cooperation

[18] http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm, March 2009

of national and (private) operator level effort. The approach at present is multi-pronged and potentially not comprehensive.

The EU may therefore play a useful role in the future to coordinate and harmonize the efforts to take protection measures to protect European critical infrastructures, to ensure designation and protection is sufficient and consistent between Member States, whilst respecting the subsidiarity principle.

3 Methodology

The IRGC Framework was used to underpin the methodology. The project was broken down in to the following Work Packages:

WP	*Title*	*Key issues to address*
WP1	**Pre-assessment**	**Identify risks under consideration, existing literature on ICT –Energy risk governance.** **Approaches to identifying ECI in ICT – Energy.**
WP2	**Risk Appraisal**	**What are the key components of risk assessment for ECI ICT-Energy?** **How should this be applied?**
WP3	**Tolerability & Acceptability:** **Risk Characterisation and Evaluation**	**What is an acceptable risk – and who should bear it? How should this be assessed?**
WP4	**Risk Management**	**What are the key options for risk management - preventative and mitigations, national and EU level implementation, decision making and monitoring.**
WP5	**Communications**	**How do stakeholders communicate and coordinate, how should this be done in the context of ECI ICT-Energy.**
WP6	**EU Risk Governance Framework Design**	**Building on all the output of WP1-WP5, we will propose a Risk Governance Framework for ECI in ICT-Energy under EPCIP.**

These work packages are described in more detail below.

3.1 Tasks

This was achieved through a Literature Review as well as a series of Project Workshops, Stakeholder Workshops and a questionnaire.

3.1.1 Literature Review

A Literature Review was carried out to collate and understand the current situation. This was carried out using internet searches and collating the information gathered by the project's technical experts.

This task addressed Work Package 1.

3.1.2 Project Workshop 1

The first Project Workshop enabled the project technical experts to:

- Contribute to the Literature Review.
- Identify the scope of the Risk Governance Framework.
- Draft questions for the Stakeholder questionnaire.
- Identify key stakeholders whom the project should engage in Stakeholder Workshops and invite to complete a questionnaire.

This task addressed Work Package 1.

3.1.3 Stakeholder Workshop 1

Stakeholders identified in the first Project Workshop were invited to attend a Stakeholder Workshop in Brussels. The purpose of this workshop was to introduce the project to these stakeholders, obtain their feedback and identify the key questions that needed to be addressed by the project.

This task addressed Work Package 2.

3.1.4 Stakeholder Questionnaire

The Stakeholder Questionnaire was refined using the feedback from the first Stakeholder Workshop and distributed to the key Stakeholders identified in the first Project Workshop. Based on the questionnaire a number of telephone interviews were used to pilot the questionnaire, but these proved to be inefficient.

This task addressed Work Packages 2-5.

3.1.5 Related EC activities

During the course of the project, Project Team members attended a number of other meetings in order to ensure that the results of this project were consistent with the other activities being carried out for EC in this area. These included:

A number of EPCIP funded projects have been conducted in parallel to this study:

- IABG led Study on Critical Dependencies of Energy, Finance and Transport Infrastructures on ICT Infrastructure.

- D'Appolonia led Study of a European Network of SCADA Security Test Centres for Critical Energy Infrastructures.

In addition, a Critical Infrastructure Protection Expert Group has been established under the EPCIP. Where possible the Project Team have kept abreast of these sister projects by attending Project Workshops.

This task addressed Work Packages 2-5.

3.1.6 Development of the Risk Governance Framework

A scoping document for the Risk Governance Framework was prepared incorporating the inputs from the previous tasks. Using this document the Risk Governance Framework was drafted.

This task addressed Work Package 6.

3.1.7 Stakeholder Workshop 2

The same group of stakeholders were invited to a second Stakeholder Workshop held in Brussels. The purpose of this workshop was to:

- Describe the draft Risk Governance Framework.

- Obtain feedback on the draft Framework from the Stakeholders.

- Test the Framework using a typical case study.

Following this workshop the Risk Governance Framework was revised to incorporate the feedback received and this Final Report prepared. This task reviewed and further refined the conclusions drawn out of the previous tasks and Work Packages.

4 Analysis

The steps shown in the methodology were carried out through the literature review, a series of meetings of the project team, stakeholder workshops and a questionnaire. The outcomes of these are described in this section.

4.1 Literature Review

The first task embarked upon by the project team was a literature review, aimed at defining the scope of the problem to be addressed and existing approaches to managing this or similar problems. The literature review firstly characterises the risks under consideration in the project by identifying the range of ICT-energy interfaces in place across Europe and their significance in terms of European energy supply. It then reviews their potential vulnerabilities, including threats and existing protection systems. Reference is made to actual incidents where possible. The literature review then describes existing procedures, programmes, policies and frameworks in use or available to facilitate the protection of particular ICT-energy interfaces deemed to be important in the European context.

The full report is included in Annex 1. Key conclusions from the report are highlighted below:

- Nowadays, national information-based CI, including electric power grids and other energy infrastructures, almost entirely rely on widely distributed and inter-operable software systems that function on the basis of open networks. In addition to increased efficiency, this exacerbates vulnerability of the infrastructures to cyber-attacks.

- Electrical power supply underlies all ICT services. Disruption to power supply is likely to cause major interruption to critical ICT services with cascading effects into other sectors of the economy.

- Chain dependencies: interdependencies may lead to unforeseen ripple effects, where the disruption of one infrastructure becomes a source of disturbance to other infrastructures. Application of effective emergency preparedness measures is therefore critically important for dealing with cascading effects.

- The dependence on information systems introduces security issues that can have a significant impact on the resilience and reliability of critical infrastructures, regardless of whether the supporting systems are centralised, standalone or embedded.

- The vulnerability of computer networks does not necessarily entail the equal vulnerability of the critical infrastructures these networks support.

- Automatic Protection Systems (APS) are intended to ensure stability of the electrical system and designed with power supplies, duplications and redundancy to minimise probability of a failure and close down from natural causes. When signalling and communications services are leased and routed through public systems, APS become open to natural, accidental, or deliberate interference.

- Until recently, the terms *process control and SCADA systems* were unknown outside their niche area in industry, and today it is one of the key issues for national infrastructure protection. These systems are becoming increasingly reliant on standard IT technologies. These technologies, such as Microsoft Windows, TCP/IP, web browsers and more pervasively, wireless technologies, are replacing proprietary technologies and further enabling the bespoke process control systems to be replaced with off-the-shelf software. This heightens vulnerability of CI to cyber attacks despite the increasing number of standards and availability of security technologies.

- The number of access points is increasing as a result of the deployment of intelligent electronic devices (IEDs), sensors, and smart meters on the grid as well as provision of remote access to systems and integration between operational and corporate business networks to support data sharing are also sources of increased vulnerability.

- Operators are often unaware of the exposure resulting from the connectivity of control systems, unsecured network connections and of the consequent vulnerability to cyber attacks. This largely results from the management's low awareness of the seriousness of the threat.

- An increasing risk to CI originates from malicious attackers who aim to expose sensitive information that can be used for state- or group-sponsored attacks of a larger scale.

- Potential threat of a cyber attack on CI can arise from nation-states using Computer Network Warfare as part of their military doctrine, terrorist groups pursuing cyber capabilities, transboundary organised criminal groups as well as insiders (employees or contractors with security access). Combination of cyber attack with physical assault can result in significant disruption and loss.

- Insider sabotage constitutes a high risk to CI. Disgruntled, demotivated or induced employees who have privileged access to ICT systems are primary sources of such risk.

- There are a great variety of tools that can be employed to launch a massive cyber attack. Such tools include worms, viruses, denial of access, unauthorised intrusion, spyware, bots and botnets and can be used in combination to initiate a compound attack.

- Contemporary CIP activities build upon a long tradition of protecting critical physical infrastructures from physical disruption. Information security professionals are seldom involved in the design, planning, implementation and management of ICT systems for the energy sector. In some cases, the security of ICT and energy systems will be handled by separate departments where personnel may use different language. The Risk Governance Framework should be applied jointly by IT and energy departments. The Risk Governance Framework cuts across different actors, different language, disconnects and considers interdependencies.

- The concepts of dependability *(ability of a system to avoid frequent and severe failures and prolonged outage durations)* and survivability *(ability of a system to fulfil its mission in a timely manner and in the presence of attacks)* are essential for protection of critical infrastructures. The vulnerability of computer networks does not necessarily entail the equal vulnerability of the critical infrastructures these networks support

- A number of initiatives have been implemented at the European level with the intention to address potential threats, including the European Programme for Critical Infrastructure Protection (EPCIP), Convention on Cybercrime of the Council of Europe, Critical Infrastructure Warning Information Network, and the explicit intention of European Commission to protect Europe from cyber attacks and disruptions.

This review was used to inform the discussions at the Project Workshop.

4.2 Project Workshop

A workshop involving all members of the Project Team was held to bring together the information held by the project team. A key purpose of this workshop was to identify and agree the scope of the Risk Governance Framework, identify the further information required through a questionnaire and the key stakeholders who should be invited to the Stakeholder Workshop and to complete the questionnaire.

The workshop discussed the context of the proposed framework. It was agreed that the level of sophistication in identifying, governing and managing risks associated the ICT / Energy interface is likely to be variable across the member states and relevant organisations operating and regulating energy infrastructures within the EU. This is likely to be compounded by the complexity of the ICT / Energy systems and networks and variations in organisational structures operating these systems across the EU, from nationalised operators (eg in newly acceded sates) through to fully privatised operational structures (as in the UK). Furthermore, management of risks were likely to be focussed on organisational (eg business continuity) or regional and national interests rather than the wider EU context. In some cases, particularly where there has been a track record of threats (either from terrorist activity or from operational perturbations) good processes were likely to be in place. It was therefore considered important that the EU is reassured that there are appropriate processes for the identification, management and governance of EC critical infrastructures and that best practices are spread to those Member States and organisations which have room for improvement.

In this context the group concluded that the proposed Risk Governance Frame work needed to:

- Provide reassurance to EU that all EU critical infrastructures in the ICT / Energy interface were adequately identified and managed.
- Ensure that where there are interconnections of energy systems between member states, all of the relevant operational and regulatory organisations are appropriately involved in the governance processes and that there are good communications for planning, operating and crisis management.
- Identify effective existing organisational, national and international governance frameworks where no further assessments may be required.
- Observe national and organisational sensitivities, so protecting commercial and national security issues and therefore be acceptable to Member States and relevant Stakeholder organisations.
- Identify best practice.
- Include realistic sharing of data, for planning, operational and crisis management as well as sharing best practices, noting the sensitivities above.

It was agreed that the scope for the Framework needed to include risks from:

- Functional failures of ICT systems and facilities including
    - Deliberate attack
    - Accidental attack (eg from random viruses) both from internal and external sources.
- Failure of the ICT system to deal with consequence of other security of supply events (eg fuel supply) - emergency response.
- Lack of capability of ICT systems to deal with major incidents.

Key ICT systems that need to be evaluated by the Risk Governance Framework included:

- Voice / fax communications.

- Data systems.
- Control and monitoring signals.
- Automatic systems (electricity protection, gas and oil - isolation and control).
- Real time operational systems.
- Data storage and archiving.
  - Ongoing operations
  - Archive
- Email.

The literature review had shown that in the past the focus has been on SCADA systems. A review of the value chains for each sector was carried out in order to establish where the key interfaces may be. This highlighted a much broader range of systems that need to be considered (Table 3.1).

	Electricity	**Gas**	**Oil**
Supply	- Coal - Gas - Oil - Uranium - (Renewables)	Import to EU - Primary production and supply	Import to EU - Primary production and supply - Pipelines and Ports
Production	- Centralised - Embedded (independent generators connect to grid, outside TSO control)	Processing	Refining
Storage	On-site storage capacity (nuclear vs gas / coal Minimal storage of electricity once generated	- LNG - Line packs - Strategic stocks (eg in old reservoirs)	Crude Products National 90 days storage
Transport	Transmission - passage through substations - interconnectors (particularly cross-border) Distribution	- Pipelines and compressor stations - Direct lines to power stations and large industrial users	Distribution via pipelines and tankers
End users	- Industrial (interruptible supplies) - Domestic uninterruptible supplies (increase in smart metering) - Commercial (banks, ICT providers) - Can be directly connected to transmission systems (eg railways) Where uninterruptible supplies are essential (eg. hospitals ICT servers etc) end users have back up generators	- Power stations - Industrial - Domestic	- Power stations - Industrial - Domestic
Control	- Real Time balancing of grid - Bidding / despatching process - Disruption would cause immediate panic - Automatic systems for control and protection - Control rooms – manual monitoring and balancing	- Remote compressor stations	
Trading systems	- Metering (billing)	- Spot markets - Bidding and balancing systems - Supply and distribution systems - Supply and distribution levels - Metering systems (affects payment systems)	- Spot markets - Refineries (usually concentrate on one supplier) - metering systems

Table 3.1: The value chain for each sector identifying possible ICT / Energy sector interfaces.

Footnotes to Table:

LNG:

- Gasification plants
- Supply feeds straight through to gas network through gasification plant
- Ports and shipping
- Storage heavily reinforced to meet safety requirements
- Trading: 20 year sales purchase system (before building plants)
- Increasing spot market (using increased capacity of plants)

In particular with the increasing use of ICT systems for operational management interfaces with business systems and then further interfaces with the wider community through public systems (including the internet) need to be considered. For example, in the electricity sector there are increasing challenges of managing embedded generation (increasing number of independent generators connecting to the grid outside of the control of the TSO's) and smart metering are likely to generate many more interfaces through these public systems.

In addition to the possible interfaces in each sector there are a number of interfaces arising at the interfaces between the energy and other critical sectors themselves:

- Active coordination of shutdowns, maintenance, unexpected loss of supply:
    - Control rooms – major users and gas supplies

- Financial systems:
    - Gas and oil prices follow each other;
    - Funding of facilities – long term investment decisions affect sustainable supplies.

- Future technical / non-technical developments:
    - Distributed networks;
    - Increasing interconnections between member states;
    - Changes in ICT technology;
        - Software developments.
        - Improvement in defences.
        - Increasing sophistication of viruses etc.

- Interfaces with ICT:
    - Dependent on electricity supply ;
    - Battery back-ups (length not defined);
    - Reliability issues.

- General communications:
    - Data;
    - Systems control (SCADA);
    - Operational control;
    - Increasing interfaces with business systems.

- Interfaces between countries:
    - Information highway for EU grid (private secure system);
    - Back-up via internet.

These issues informed the design of the questionnaire and the agenda for the first Stakeholder Workshop.

4.3 Stakeholder Workshop 1

The objective of this workshop was to introduce the project, and the proposed Risk Governance Framework to key stakeholders, and to receive feedback on them to confirm the scope of the project. Workshop sessions on Energy / ICT Interfaces, existing Risk Governance Frameworks and coordination and communications were used to confirm our initial conclusions and refine the questionnaire.

About 150 people were invited to the workshop: 34 people attended from a range of Member States and representing organisations in each energy sector. The notes of the meeting, the organisations and countries represented, as well as the main presentations made are included in Annex 2.

The main outcomes from the meeting were:

- The Risk Governance Framework needs to be integrated in other security management processes that are applied in energy systems. The framework needs to complement the Risk Management systems that are already in use, e.g. for security of supply.

- Incorporating the Risk Governance Framework as a mandatory element of the Operator Security Plan (OSP) may not be feasible given the OSP confidentiality restrictions that will hinder sharing of information and best practice. Moreover, the OSP is intended for energy CI only and does not include ICT.

- The Risk Governance Framework should distinguish between internal ICT systems (solely used for the purposes of energy sector) and other ICT market systems.

- The Risk Governance Framework should cover the knock-on effects beyond disruption of supply.

- Given that ICT providers implement cyber security improvements, their involvement in implementing the Risk Governance Framework is important.

- Most ICT systems are not highly critical at any stage of the supply chain thanks to redundancy that has been built up, e.g. manual switching.

- If suspended, some ICT systems may cause an impact in one country but a 2nd country effect is unlikely.

- In case of a control system failure, transportation of electricity and gas is still possible but the operators’ ability to control the flow diminishes, whereas the probability of supply disruption increases.

- Remote control and accessing information in real time via the internet is likely to become of greater importance to end user exchanges and advanced metering.

- There remain companies that still continue using internet based SCADA systems without realising their vulnerability.

- Insider attacks, either accidental or deliberate, remain amongst the most significant threats, together with a risk of organisational failures and internal interdependencies.

- Various defence mechanisms help manage the ICT related risks and reduce the likelihood of an incident. Such mechanisms include early warning systems, security policies and procedures, vetting of personnel and suppliers, system design defence, physical security barriers, email and web defence.

- Smart grids and generation of renewable energy, including embedded generation, increase data handling and tend to result in less predictable levels of despatch.

- Smart metering is likely to increase the vulnerability of the ICT system providing access points in individual households.

- Informal arrangements between operators are essential in enabling flexibility and promptness in the crisis management situations.

- Commercial interests and sensitivities tend to hinder information sharing. Ways of enabling safe sharing of the relevant information and best practice should be explored.

- A shift from national to international level is needed in the entire concept of infrastructure protection. Mechanisms for international cooperation should be considered.

- Member States should be incentivised to identify ECI in other countries. This will lead to better understanding of the existing responsibilities in the ECI remit.

The level of preparedness seems to be variable across Member States reflected by level of engagement in project. EC will need to be sensitive to this in introducing and using RG framework.

In particular, some companies say they have well developed CI protection systems and are wary of EU involvement in their processes. None the less the Banking crisis demonstrates the requirements for national and regional governments to be reassured that this is the case and understand where there may be gaps. It is also their role to ensure that communications between the key actors are efficient both in terms of planning (prevention and mitigation) and in crisis management. In particular, it is the role of the EU to ensure that it can facilitate this communication and bring standards up to a common acceptable level to ensure supplies across EU by identifying weaknesses and transferring best practices.

It was felt by the stakeholders that a representative from each country should identify, using the Risk Governance Framework or using its own processes, the key critical infrastructures:

- In neighbouring Member States which that country depends on for its supply.

- In its own country which it considers are critical to the EU network.

By comparing the results of these analyses, it will be possible to identify a common understanding of the key infrastructures, understand where there are differing perspectives on which are critical infrastructures. Where there are disagreements the Risk Governance Framework can be used as a common approach on which to frame a dialogue to resolve differences. Where there are common understandings the Risk Governance Framework can be used to further characterise the risks and develop appropriate plans for the prevention and mitigation of risks, as well as developing communication plans, for each of the infrastructures identified.

Representatives from Member States (eg Ireland and Portugal) at the geographic peripheries of the community (and therefore at the end of the transmission lines), were particularly keen for the EC to have a mechanism to ensure security of supply.

4.4 Questionnaire

The questionnaire is provided in Annex 3. It was distributed to the same stakeholders invited to the first stakeholder workshop. These represented government organisations, and a wide range of organisations representing all of the energy sectors as well as IT specialists, from each of the EU Member States. We received 16 responses (see annex 3 for the organisations and countries represented). While this is a relatively small number of responses, it does represent a number of countries and energy sectors.

Figures 3.1 – 3.3 summarise the findings for the electricity and gas sectors

Figure 3.1 Average Criticality Score - Electric

	Primary production and supply (gas liquefaction plant for LNG)	Import to EU and supply - Pipelines and ports	Storage	LNG - regassification	Processing	Transportation	End users – power plants	End users - major industrial	End users - all others	Energy metering and financial settlement	Energy trading
Voice communication (fixed and/or mobile telephone) (via shared public systems)	4.0	3.3	5.0	4.0	4.0	3.5	3.7	4.0	4.0	2.3	4.0
Voice communication (fixed and/or mobile telephone) (via private systems or dedicated leased services)		1.5	4.0	5.0	4.0	3.0	4.0	4.0	3.0	3.5	
Written communication (fax and/or email) (via shared public systems)	5.0	3.7	5.0	2.0	3.5	3.7	3.3	3.7	4.5	3.5	5.0
Written communication (fax and/or email) (via private systems or dedicated leased services)	5.0	3.0	4.0		4.0	4.5	4.0	4.0	3.0	4.0	
Remote control and accessing information in real time using the internet	5.0	5.0	5.0		4.0	5.0	4.0	5.0	4.0	2.0	
Remote control and accessing information in real time using private networks	5.0	2.5	4.0		4.0	3.0	4.0	4.0	3.0	2.5	
Automated operation and control (SCADA systems) (general internet based)	4.0				4.0	4.0					
Automated operation and control (SCADA systems) (via private systems or dedicated leased services)	5.0	3.5				3.5	5.0	5.0		2.0	
Automated data logging and metering (general internet based)	5.0	3.0	3.0		4.0	3.0	3.0	4.0	4.0	3.0	
Automated data logging and metering (via private systems or dedicated leased services)	5.0	2.0	3.0	5.0	4.5	2.8	2.0	2.5	4.0	2.5	
Safety real time high speed protection systems (via public/shared external systems)		2.5	4.0		4.0	2.5	2.5	3.0	3.0	4.0	
Other (please specify in space below)											

Legend: High Criticality = 5 Low Criticality = 1

Figure 3.2 Average Criticality Score - Gas

	Fuel purchase and supply	Centralised generation providing main and ancillary services	Embedded and intermittent generation	Real time system balancing and generation dispatch	Transmission	Distribution	End users – providing ancillary balancing services	End users – Critical services to ICT Sector	End users – Critical services to other energy sectors	Energy metering and financial settlement	Energy trading
Voice communication (fixed and/or mobile telephone) (via shared public systems)	4.0	2.3	4.0	2.8	3.0	2.5	3.3	4.5	2.0	2.3	2.7
Voice communication (fixed and/or mobile telephone) (via private systems or dedicated leased services)	3.0	3.0	3.3	3.3	3.8	3.5	4.0	3.5	2.0	2.3	2.7
Written communication (fax and/or email) (via shared public systems)	4.0	1.7	2.7	2.5	2.6	2.0	2.5	4.5	2.0	1.3	3.0
Written communication (fax and/or email) (via private systems or dedicated leased services)	4.0	2.3	2.0	3.0	3.2	3.0	2.5	3.5	2.0	1.3	2.3
Remote control and accessing information in real time using the internet		1.7	2.7	2.5	2.4	2.5	3.5	4.5	2.0	1.5	3.0
Remote control and accessing information in real time using private networks		3.7	3.3	4.3	4.4	3.5	3.5	3.5	2.0	1.3	2.7
Automated operation and control (SCADA systems) (general internet based)		3.0	4.0	3.5	3.5	2.0	3.5	4.5	2.0	1.5	1.3
Automated operation and control (SCADA systems) (via private systems or dedicated leased services)		3.7	3.3	4.3	4.4	3.0	3.5	3.5	2.0	1.5	1.3
Automated data logging and metering (general internet based)		1.7	2.7	2.5	2.4	2.0	3.5	4.5	2.0	1.5	2.3
Automated data logging and metering (via private systems or dedicated leased services)		2.3	2.0	3.0	3.0	3.0	3.5	3.5	2.0	1.5	2.3
Safety real time high speed protection systems (via public/shared external systems)		3.0	4.0	3.8	4.2	2.0	3.5	4.5	2.0	1.5	1.3
Other (please specify in space below)											

Legend: High Criticality = 5 Low Criticality = 1

Figure 3.3 Pan European Approach to Risk Governance of the Energy/ICT Interfaces – responses to question 4

Can the Risk Governance Framework:	Average score	Standard deviation
Provide a mechanism to assess the risk governance methods used in EU Member States.	1.7	0.6
Provide a mechanism for application of best practices found in EU member states to certain critical infrastructures.	1.7	0.6
Through a common framework provide a high level interface to existing national risk governance arrangements for communicating results of risk assessments to Commission and to other MS.	2.2	0.8
Provide a mechanism for identifying and quantifying risks that affect energy supply in more than one MS.	1.9	0.5
Provide a mechanism for identifying and assigning responsibility for risk governance issues where this is not currently clear.	1.9	0.7
Provide a mechanism for MS to identify best practice from across the EU when assessing and revising existing systems and procedures operating at national level.	1.6	0.6
Formally recognise risks at the interface between ICT and energy systems that have not been addressed by previous work (either at EU level or nationally or by industry participants).	2	0.7
Provide a concise summary of the types of risk that should be considered by authorities in individual MS and industry participants, and how these might change in the future as the energy and ICT sectors change (e.g. increasing reliance on digital control systems, increasing interconnectivity between private networks and the internet).	1.8	0.9
Provide a concise summary of the types of defences that should be considered by authorities in individual MS and industry participants (physical security, ICT system design, maintenance and operation, disaster recovery, etc).	2.1	0.9

Legend: Agree Strongly = 1 Disagree Strongly = 4

For the electricity sector most respondents identified the following key ICT interfaces:

- Remote control and accessing information in real time using private networks, for:
  - Real time system balancing and generation despatch;
  - Transmission.

- Automated operation and control (SCADA systems), via private systems or dedicated leased systems for:
  - Real time system balancing and generation despatch;
  - Transmission.

- Safety and real time high speed protection systems (via public/shared external systems) for:
  - Transmission;
  - End users – critical services to the ICT sector.

In addition to these a range of ICT interfaces are key in energy metering and financial systems and for some end users – providing ancillary balancing services.

This highlights the importance of managing ICT interfaces with both private and public networks. In addition, it was noted that private networks can have interfaces with public networks.

For the gas sector most respondents identified the following key ICT interfaces:

- Import to the EU and supply pipelines and ports.
- Isolated interfaces in all parts of the value chain from processing through to end users Contrasting with the electricity sector Energy was not considered to be important (presumably because of the difference in time frames required for this).

The most critical interfaces were identified as being in the primary production and supply. All forms of ICT systems were considered to have critical interfaces with the various processes in the value chain. As with our previous study this highlights the importance of the supply chain outside of the EU.

There were insufficient responses in the Oil sector to carry out an analysis, but it is likely that the results will be similar to those of the gas due to the similar timescales and characteristics.

Other key conclusions drawn from the questionnaire were:

- General agreement that the framework will be useful for its defined purpose (cross-border, good practice, consistent approach, identifying types of risks).
- Mixed views (disagreement 6/14, agreement 8/14) that the framework can provide a high level interface with existing national risk governance arrangements for communicating results with commission and other Member States.
- Mixed views (disagreement 4/15, agreement 13/15) that it will provide a concise summary of the types of defences that might exist.
- There is no recommendation of who should be mandated to use the framework (but a recommendation of it being carried out at a Member State and organisation level, and at the EU level (providing assurance).
- We discovered that if a stakeholder is dependent on others for energy supply then they were interested in using the Risk Governance Framework (to identify risks from further up the supply chain). If a stakeholder is within the middle or at the beginning of the energy supply chain then they are not so worried about (having) to use the Risk Governance Framework.
- There seem to be a small number of organisations who have defined procedures for a risk governance process and processes for assessing the risks and dealing with them – however most organisations who responded used ‘ad hoc methods without formal guidance’.
- The majority of stakeholders verified the use of the ISO standards for ICT including requirements, code of practice, and risk management (ISO/IEC:27000 series). There are also (international) organisations that have their own specific approaches and publicise these.

4.5 Related EC Activities

A number of EPCIP funded projects have been conducted in parallel to this study:

- IABG led Study on Critical Dependencies of Energy, Finance and Transport Infrastructures on ICT Infrastructure.
- D’Appolonia led Study of a European Network of SCADA Security Test Centres for Critical Energy Infrastructures.

In addition, a Critical Infrastructure Protection Expert Group has been established under the EPCIP. Where possible the Project Team have kept abreast of these sister projects by attending Project Workshops. Key findings from these projects of relevance for this project are provided here.

European Network of SCADA Security Test Centres for Critical Energy Infrastructures.

Key points of relevance raised at the Project Workshop are:

- A Risk Governance Framework will be useful to member states so that they can confidently define the possible attack/threat scenarios, which in turn can be considered by a SCADA test centre to ensure that tests are comprehensive.
- Managing the implementation of any necessary security patches in a 'live' energy supply system creates risks to supply.
- Any system or component vulnerabilities which have been identified by tests must be treated with secrecy (risk of falling into the wrong hands).
- The security characteristics of interoperability with 3rd party equipment needs to be understood: this is a potential area of risk.
- A whole system life cycle approach to security is required and security training at all stages of a system's lifecycle is required.
- Security needs to be embedded within the organisation's governance and behaviour, not as an add-on. It is a costly exercise to design and test for security, this needs senior level support.

Critical Infrastructure Protection Expert Group

One CIP expert group has been established so far focussing on ICT and electricity sector interdependencies. This meeting highlighted that this is a developing area where there are a number of technical developments and research tasks being carried out. Member States are developing their own systems for identifying and managing risks at organisational and national levels (eg. Sweden's interactive tool for dependency analysis). It would be useful for EU to have a practical tool for identifying these best practices and ensuring that EU critical infrastructures are properly assessed.

Study on Critical Dependencies of Energy, Finance and Transport Infrastructures on ICT Infrastructure

The team participated in both the initial and final workshops of the project.

The ICT / Energy interfaces identified in both projects were similar.

In the electricity sector transformers, control centres and frequency / load control systems were identified as being high-risk interfaces. It was noted that care needed to be taken in defining private and public ICT systems because dedicated lines were sometimes rented from public utilities and systems may pass through non-dedicated router systems – this reinforces our observation that different actors use different languages and these defined clearly when carrying out the Risk Governance process.

For the gas sector key infrastructures were identified as compressor stations, control centres, pressure control systems and export stations (containing compressors and mixers). While control systems are currently routed via private systems it was felt that there was an increasing trend to use public systems even though this was seen, at the moment to be bad practice. It was noted that a completely destroyed compressor station would take over 2 years to rebuild but that there is work to mitigate this type of loss by enabling reverse flow in some pipelines (currently very few pipelines are enabled to do this, but it is changing).

It was noted that the recent disputes affecting the supply of gas through Ukraine had not caused a "critical" event in EU.

Care needs to be taken in using the EPCIP guidelines for Hazard Categories because the definitions of the categories are sufficiently large that it is unlikely that there are many infrastructures (or combinations of events) in the energy sector which would cause a significant EU event in these terms.

Our conclusions are that analysing the economic and social consequences of a disruption caused by a significant energy disruption is problematic. It is likely not only to be affected by the real impacts of the loss, but also by the perceptions surrounding such a loss. In categorising the risks as “complex” or “simple” the IRGC framework provides some information on how these Hazards should be further investigated, but we have recommended further work to address this complex issue.

The final workshop summarised the following key ICT dependencies in the energy sector:

- IT system/services - SCADA/process control (Electricity, Oil and Gas), messaging service (Electricity), file transfer service (Electricity).
- Communication systems – private LAN and WAN networks (Electricity, Oil and Gas).

Periods of heightened concern include those where software updates or upgrades are being performed, where software support (hotline, remote access) is required or when remote maintenance is being carried out. It was noted that protection technologies are almost always available to mitigate risk but are not always used. This reinforces the need for a Risk Governance structure to establish a common level of risk acceptability and standards for risk management.

Several ongoing developments in ICT and the energy sector are likely to increased risk:

- Increased connectivity.
- Increased wireless networks.
- IP based network communication.
- Broadened use of commodity IT platforms.
- Cloud computing.
- System complexity.
- Smart grids.
- Grid dynamics.
- Regulatory requirements.

The IABG study found that all sectors invest heavily in build-up and operation of redundant ICT systems. However protection or mitigation capability is weak with regard to “new” ICT-threats despite the fact that sophisticated degradation modes are available to mitigate such vulnerabilities. These findings align very well with the ‘precursors’ discussed in the Risk Governance Framework developed by this project and summarised in the Conclusions section.

4.6 Stakeholder Workshop 2

The objective of this workshop was to introduce the draft Risk Governance Framework, to obtain feedback from the stakeholders and test the framework by working through an example to test it.

The same set of stakeholders were invited to the workshop ,12 people attended from a range of Member States mostly representing their government’s critical infrastructure protection organisations (see annex 4). The notes of the meeting and main presentations made are included in Annex 4.

There was a positive reaction to the Risk Governance Framework and it was considered by the participants to be practical to use. They liked the categorisation of risk in to complex, uncertain, ambiguous and simple, since this enabled differing actors to be identified in developing appropriate action plans to manage these different types of risk. It was also considered relevant to consider the wider social consequences of failures, but that it was considered that this should be separated out from the technical / functional risk assessment since it was recognised that this required a different range of knowledge / skill set to the technical / functional assessment. It was therefore agreed that this should be a separate stage of the impact assessment carried out in the Characterisation and Evaluation phase.

The feedback on the proposed Risk Governance Framework included a recommendation that more detailed guidance should be provided on identifying complexity and ambiguity of a problem as well as on assessing uncertainties and dealing with unpredictable risks.

Other comments and conclusions included:

- Inter-country interdependencies and associated vulnerabilities tend to be underestimated in practice.

- Smart metering systems may affect the risk management. The IRGC framework allows actors to identify important trade offs, e.g. between energy efficiency and security.

- Prediction of risks is not always easy as eventual hazards may differ from initial assumptions.

- Assessment of social consequences should be a separate initiative. Social impact may be difficult to measure on the same scale as the energy supply impact. However, the weighting and magnitude of social impacts may be equal or even exceed those associated with the impact of supply loss.

- On the vulnerability scale, strength of defences is of more importance than frequency of a threat.

- It is significant to identify redundancy and secondary redundancy communication systems to be employed in case of a system disruption. Given that mobile, fixed and internet telephony often use the same infrastructure, it is important whether the redundant telephony function is a separate standalone infrastructure. Availability of a fixed line would not prevent disruption to electricity supplies that are typically immediate.

- In the past, there was a tendency to use private leased lines for communication purposes. In pursuance of cost efficiency, the present ICT provisions are often internalised and rely on public internet connection. This practice may serve as a precursor for increased risk.

- The crucial communication lines are those connecting SCADA systems to the TSO national control centres.

- Data storage is also a component of the SCADA system. Data exchange and communication occurs between neighbouring operators, not only between an individual operator and SCADA.

- Functional disruption of a control system does not necessarily result in the cessation of energy flow but leads to the operators' inability to respond.

- Temporal aspects of a disruption/ failure should be given consideration, in particular – time of year and duration.

- It is important to identify common mode failures which can occur for a variety of reasons, for example, where the same technology has been adopted and also where systems rely on a common power supply, common input data source, are maintained or tested by the same person, use components from the same batch or design that may have a weakness etc are located physically close to each other or are at risk from some common event e.g. flooding, seismic event, etc.

- Automatic Protection Systems (APS) are not always ICT related. The exception is digital APS in SCADA.

- In case of a trading system failure, energy supply continues at the last agreed rate. In such a situation, however, there remains a possibility of bottlenecks forming in the supply chain.

- The main actors in the ICT-energy interface are:

    - **EU Level**
        - EC (DG JLS, DG Tren).
        - CIP Expert Group.
        - European Trade Associations.
        - European Network and Information Security Agency (ENISA).
        - Transmission System Operators (who do not necessarily align with national borders).
        - ENTSO (Electricity).

    - **National Level**
        - Government Department / ministry responsible for energy / ICT security.
        - National organisations responsible for protect critical national infrastructures.

    - **Company Level**
        - Multi-national organisations.
        - National Organisations.

- Relevant actors need to have the appropriate responsibility and expertise to execute necessary actions. Therefore, involvement of management along with technical and risk experts is needed.

- Possible precursors to risk events are system variations (including exogenously imposed changes), alterations to the types of technology and software, the lack of prior testing, insufficient ICT/security awareness among the management and in the overall organisation’s culture, terrorist awareness of criticality/ vulnerability of a particular infrastructure.

- The language used to describe ICT systems is not consistent. Different people use different terminology and in particular energy technologists do not use the same language as ICT experts. In practice, this is not a problem since the terms can be defined during the Risk Governance process so that a common understanding is achieved.

5 Risk Governance Framework

5.1 Introduction for Member States

There are four questions concerning the use of a Risk Governance Framework in Europe:

- Why is a Risk Governance Framework required?
- What is the purpose of the framework?
- Who should be interested in using the framework?
- How should the framework be used?

The following material answers these questions, providing supporting evidence from previous work and from the questionnaires and workshops conducted during this study. A simplified version outlining the steps in the framework without the extended commentary is provided in Annex 5.

5.1.1 Background

In December 2008 a Directive on the identification and designation of European Critical Infrastructures (ECI) was adopted. The Directive lays down a procedure for how to identify ECI. In summary:

- ECI are those infrastructures, the destruction or disruption of which would affect two or more Member States, or a single member state if the critical infrastructure is located in another Member State.
- Cross-cutting criteria have been proposed that would be used to identify which infrastructure was critical from the point of view of the potential impact on EU citizens, the economies in the Member States, etc. These criteria would apply to all sectors.
- Additional criteria can also be identified that are specific to particular sectors (energy, transport, etc).
- Each Member State would then identify those infrastructures that satisfy the criteria and notify the Commission of those national infrastructures identified in each sector.
- Owner/operators would be required to establish an Operator Security Plan to identify and rectify any security gaps that are identified.

The Energy sector has been identified as high priority, and work is already on-going to assess critical infrastructure in the EU production and distribution/transportation systems for oil, gas and electricity. The ICT sector is also a high priority ECI, including for example EU data and voice services across both fixed and wireless networks. However, the energy industry is particularly dependent on ICT systems so there is an important interface between the two sectors that needs to be understood in the context of the Directive.

5.1.2 Purpose

The primary purpose of this Risk Governance Framework is therefore to focus on the decision making processes in EU member states for dealing with the risk of disruption to cross-border energy supplies that can arise from ICT related incidents.

The aim is to provide a consistent approach to decisions affecting the Energy-ICT interface, using best practice risk governance theory.

The Risk Governance Framework provides a standardised approach for quantifying and managing risks to cross-border energy supply. It is based on an analysis of what is already being done by infrastructure operators and Member State governments either unilaterally or through existing bi-lateral or multi-lateral arrangements and what needs to be done to bridge any gaps. The framework defines a minimum standard to be achieved but must also allow flexibility in how it can be applied in each Member State and organisation to fit local practice.

This definition of purpose was tested and validated during the first workshop and follow-up questionnaires (see Section 4.3). There was strong support for a mechanism to benchmark the risk governance methods used in EU Member States and to facilitate the spread of best practice, but much less support for requiring the results of national risk assessments to be communicated to the EU using the framework as a common language. This is a sensitive area and issues of confidentiality needs to be identified and overcome. Nevertheless, the EU as an important stakeholder in the process would presumably wish to become better informed of the cross-border threats that exist through the application of the process by each Member State.

The Risk Governance Framework is designed to be used by Member States to consider the current risks, but if required, it can also be used to assess potential future risks.

5.1.3 Potential interested stakeholders

The primary audience for the Risk Governance Framework is the Government of each Member State and their energy producers, energy distributors/shippers and energy network operators where it is applied. It is likely that in this context the framework would be used at a national level by individual organisations to highlight any **cross border** criticalities between Member States. The EU commission would also have a key interest in any such cross border criticalities and there may also be linkages with reporting under Directive 2008/114/EC[19]. At present, under the Directive, Member States are required to report the following to the European Commission:

- The number of infrastructures per sector for which discussions have been held concerning the identification of EU critical infrastructures for the energy and transport sectors (annual reporting).

- The number of designated ECIs per sector and the number of Member States dependent on each designated ECI (annual reporting).

Member States are also required to:

- Inform other Member States which may be significantly affected by a potential ECI about its identity and reasons for designating it as a potential ECI. Member States are also required to engage in discussions with other such Member States.

- Inform the operators of infrastructures designated as ECI, to determine whether an Operator Security Plan is in place for ECI and if not to ensure and OSP is put in place and regularly reviewed within one year of designation as ECI.

- Report to the Commission generic data on the types of risks, threats and vulnerabilities encountered per ECI sector in which ECI have been designated (biennial reporting).

[19] Directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection.

The Commission's stated role is to:

- Facilitate and participate in discussions between Member States where necessary.
- Assess with Member States whether further protection measures at a Community level should be considered.

The Risk Governance Framework is expected to be used by Member States, energy producers, energy distributors/shippers and energy network operators to identify any ICT / energy critical interfaces which affect **cross-border** energy supply, and report this to the EU.

However, the Risk Governance Framework could also be used at a national level by Member States. They will be able to coordinate input from individual organisations to highlight any **cross boundary** criticalities within a single Member State. It is hoped that this will encourage infrastructure operators and Member State governments to contribute to the creation and use of the Risk Governance Framework.

The framework could also potentially be used by significant **energy customers** to help them challenge their suppliers with pertinent questions about the security of their energy supply to ICT related incidents.

5.2 The context of the Risk Governance Framework

Before describing the individual steps of the Risk Governance Framework, it is important to explain some of the context in more detail, in particular:

- What is meant by the energy / ICT interface and therefore what is within the scope of the decision making process.
- What is the meaning of the term 'cross-border' and how the framework could also be used to understand cross-boundary issues between organisations and departments.
- An outline of the four main steps in a generic Risk Governance Framework, and
- The mix of the different roles and responsibilities of those who would add value to the decision making process, and who therefore should be involved in its application.

5.2.1 Scope

The framework considers the interface between ICT systems/processes and energy systems/processes for electricity supply, natural gas and LNG supply, and oil supply including oil based fuels (refined products). Coal supply is outside the scope of the framework because it was considered that ICT systems are not fundamental to this supply chain. However, the framework could be used in this context where cross border issues are particularly important for some Member States.

It does **not** consider ICT systems external to the energy supply chain (i.e. those systems where a failure would not impact the ability of the organisation to play its part in the flow of energy, such as company web sites for the general public or other non-energy businesses operated by the same organisation, provided that these do not provide an 'entry point' into the energy business itself).

It considers the energy supply chain from primary production through storage, transmission and distribution/transportation to metering and financial settlement, but it does **not** consider any ICT/energy interfaces within the premises of the final energy consumer.

It considers threats arising from anywhere in the world that affect one or more industry participants operating within one or more Member States.

It considers threats arising from:

- Inadequate ICT system design, implementation or maintenance.
- Deliberate or targeted cyber attacks on a particular system or organisation.
- Accidental or non-targeted exposure to viruses, worms etc.
- Failure of third party ICT systems (e.g. mobile telephone).
- Inadequate ICT capability to respond to energy supply incidents from other causes.
- Inadequate emergency response and disaster recovery of failed ICT systems.

It does **not** consider the effects that failures of energy supply from other causes might have on ICT systems outside of the energy industry (e.g. the impact of electricity supply failure on the ICT systems used by financial institutions or hospitals).

The criticality of the energy/ICT interface depends on the scale of the energy supply disruption and the length of time it takes to return to normal. The framework does **not** attempt to convert this into a direct financial loss or to quantify other social or environmental consequences arising from the loss of supply. The EU Directive has already classified the energy infrastructure as a priority sector, so by definition an interruption to energy supplies is likely to have a material financial or social outcome. If required an individual Member State could add its own conversion factor to express the energy disruption outcomes in financial terms, but our research for the previous energy ECI project concluded that this was impossible to do in generic terms because it was so dependent on the types of businesses that were affected by the disruption. The only common currency that is sensible to use for comparisons between Member States is the length of time for which energy is disrupted. This is the basis of the consequence scale we have suggested. Further guidance on this can be found within the other EU ECI work streams, in particular:

- AEA led 2007 Study on Definition of Critical infrastructures at EU level in the energy sector.
- IABG led Study on Critical Dependencies of Energy, Finance and Transport Infrastructures on ICT Infrastructure.
- D'Appolonia led Study of a European Network of SCADA Security Test Centres for Critical Energy Infrastructures.
- Booz and Company led Study on Stocktaking of existing critical infrastructures protection activities.

5.2.2 Clarification: Use of framework for cross-border and cross-boundary ICT/energy interfaces

To ensure that the Risk Governance Framework has the maximum possible benefit to a wide group of stakeholders, it should be flexible so that each stakeholder can consider risks within their own areas of responsibility. For example, at the EU level, managing the risks to cross border energy supply is the key driver for the use of this framework. At Member State level, a network operator may wish to manage risks across other boundaries that are not necessarily cross-border.

Therefore, the Risk Governance Framework is able operate at any of the following levels, and the first part of the application of the framework includes an identification of which level is appropriate.

- **EU cross-border**. Where an ICT system functional failure disrupts energy supplied in one Member State from reaching another Member State, or where the disrupted energy flow transits across a Member State en-route to its final destination.

- **Non-EU cross-border.** Where an ICT system functional failure in a non-EU country affects the flow of energy into a Member State.

- **Member State national**. Where an ICT system functional failure in one part of the country's national infrastructure affects energy supply to a significant proportion of the population within a single Member State.

- **Inter-organisational.** Where an ICT system functional failure in one organisation affects the operations of another organisation resulting in energy supply disruption within a single Member State**.**

- **Intra-organisational.** Where an ICT system functional failure in an energy company's own operations results in an energy supply disruption within its host Member State.

5.2.3 Outline

The Risk Governance Framework is a high level document that describes a flexible process. It aims to provide helpful guidance and a set of tools and checklists to assist a user in assessing and managing risks, and to communicate effectively.

The complete framework and example checklists and templates are provided in Annex 5, in a format that could be separately published as an electronic document or hard copy brochure. Example case study applications are also provided in Annex 6.

This section of the report provides a more detailed annotated commentary on each step in the framework, to explain the reasons for the conclusions that were reached and to provide supporting evidence where this is available from the workshops and questionnaires that were conducted.

The generic approach to risk governance developed by the IRGC is being used as a template structure for this process. This template breaks the activities in the process into the following five elements.

- **Pre-assessment**; which involves getting a broad picture of the risk.

- **Appraisal**; which identifies the knowledge needed for judgement and decisions.

- **Characterisation and evaluation**; which assesses whether the risk is acceptable or not.

- **Management**; which identifies who needs to do what and when.

- **Communication**; which determines who needs to be told, when and how.

The energy/ICT Risk Governance Framework guides the user through four stages of pre-assessment, appraisal, characterisation and evaluation, and management. At each stage it prompts users to consider the fifth element of communication.

These steps can then be repeated to provide a basis for continual improvement.

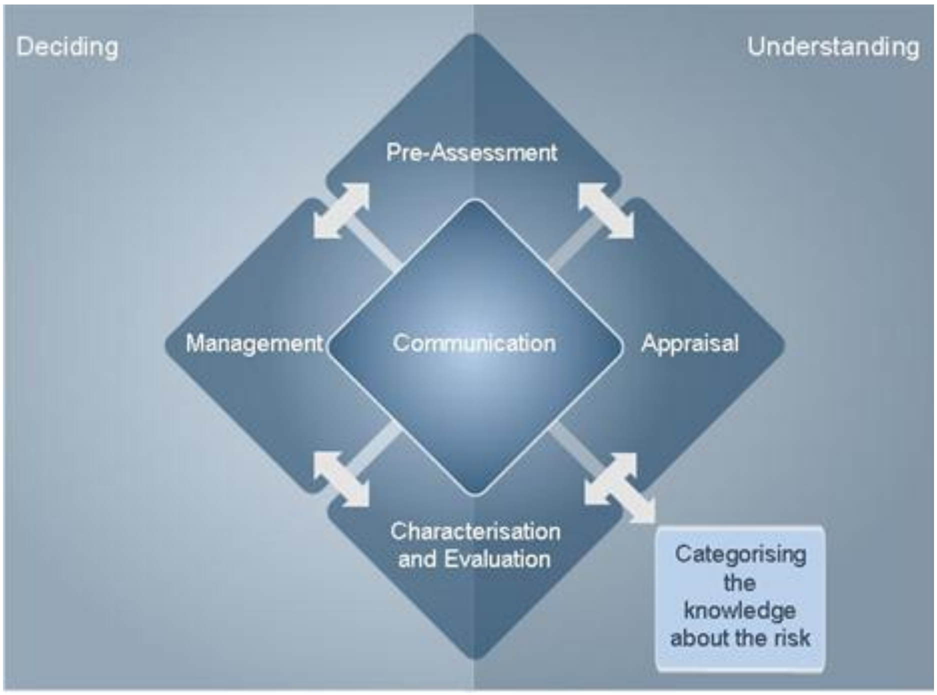

Deciding
Understanding
Pre-Assessment
Management
Communication
Appraisal
Characterisation and Evaluation
Categorising the knowledge about the risk

Figure 3: IRGC Risk Framework

One important dimension of the IRGC framework is the inclusion and treatment of the socio-cultural dimension of risk - how civil society (the public and governments) understands the risk and participates in the risk governance process. IRGC refer to this as concern assessment. This is a complex area of analysis and the annotated framework below contains a discussion of the extent to which this analysis has already been considered by the European Commission in defining the Energy infrastructure as a priory sector in the first place. However, once priority critical interfaces between the energy and ICT infrastructures have been identified, member states need to have the flexibility to undertake a more thorough concern assessment for their own local circumstances. For example this might include a decision to undertake a more detailed study of the economic and social impacts of the risks in order to provide more evidence for the attractiveness of further risk reduction measures.

5.2.4 Roles and Responsibilities

It is for each member state or organisation to decide who should be responsible for the application of the Risk Governance Framework, and for pursuing its outcomes to reduce any identified vulnerability. However, an example of best practice for an organisation might include the following:

- A senior director or senior manager to sponsor the activity and give it the necessary authority within the organisation.

- A risk manager who is an expert in the process and who can act as an internal consultant. This person would also usually take on responsibility for maintaining the master version of the risk register, tracking the progress of any agreed risk management actions that arise, and communicating the results of the risk assessments to other stakeholders such as the other parties involved in any cross border or cross boundary criticalities that have been identified. Potentially, the risk manager would also be responsible for communications with the EU Commission.

- Energy and ICT infrastructure professionals would be responsible for identifying and evaluating the interface risks using the framework. This is best done as a collective exercise, for example in a series of workshops. The risk manager may be called upon to facilitate the workshops if necessary.

- Experts may be required to fully quantify the political, economic, and social impacts of energy disruption if a more detailed impact and concern assessment is undertaken within a Member State. This goes beyond the qualitative risk ranking scales proposed here.

- Where further risk reduction measures are required for particular critical interfaces, the responsibility for delivering the agreed action plan should reside with the person best able to deliver it in each case.

The launch of the risk governance process, the pre-assessment phase, needs to include participants who can represent all of the above roles and responsibilities as a minimum. Additional participants should be identified and invited to join as the risk governance proceeds.

5.3 Pre-assessment Phase

IRGC: Early warning and "framing" the risk in order to provide a structured definition of the problem, of how it is framed by different stakeholders, and of how it may best be handled.

Good risk governance starts with defining the scope of consideration and gathering information about stakeholders' responsibilities. This ensures that there is a common definition of the topics to be considered, and that all actors involved in the risk management process understand their role. Good preparation and definition makes for a more efficient risk management process.

Pre-assessment task 1

TASK: Define the interfaces between the energy and ICT systems which are potential targets and need to be considered in the risk governance process. These are the interfaces between energy and ICT systems that if compromised could cause a disruption to cross-border energy supplies.

This task should consider the ICT systems that both directly affect cross border energy supply, such as a control system, but also systems which could indirectly affect energy supply, such as a business system. The types of systems considered should therefore include:

Operational and Safety Communications: Without this communication under fault conditions and no supply conditions, failure of communications will delay work taking place to restore services and system integrity. Examples include telephone (fixed or mobile), fax and email.

SCADA and Network Management Systems, providing control and monitoring of plant. Communication is required most critically under abnormal system conditions. Examples include manual or automated remote control via private networks or the internet.

Automatic Protection Systems: These systems detect faults and disconnect services quickly to ensure stability of systems. Failure to clear a single fault can close down all or part of systems and its interconnections. Examples include automated system control via private networks or the internet.

Data: Data is fundamental to correct operation of ICT systems both under normal conditions and also critically under abnormal system conditions; current and forecasted demand and supply of services, planning information, plant status information. Data corruption, or lack of access to required data can disrupt the balance of a system, implemented control measures and recovery may be delayed.

An example of an electricity energy sector supply chain:

- Fuel purchase and supply;
- Centralised generation providing main and ancillary services;
- Embedded and intermittent generation;
- Real time system balancing and generation dispatch;
- Transmission;
- Distribution;
- End users – providing ancillary balancing services;
- End users – Critical services to ICT Sector;
- End users – Critical services to other energy sectors;
- Energy metering and financial settlement;
- Energy trading.

It is also important to consider systems and data throughout the supply chain. Annex 7 provides a matrix with a generic list of all the potential ICT interfaces for the electricity, oil and gas supply chains. These matrices were tested for relevance and completeness during the questionnaire process, see Section 4.4. These matrices can be used to identify the critical ICT / Energy interfaces.

Of course, systems can be described at different levels of detail. To ensure that this process is practical the highest level of system detail should be chosen, for example;

- a control system (including PC/laptop control interfaces, networks, control actuators and measurement devices),
- an email system (including PCs/laptops, networks, servers and data storage),
- a telephone system (including handsets, network terminating units and telecoms networks).

More detailed descriptions of systems, broken down into individual components, may reveal additional threats to be considered. Systems can be represented at these lower levels of detail if required.

Table 1 (Annex 5) provides a template for recording this list of critical interfaces that may be threatened; these are the systems which are potential targets for attack.

Pre-assessment task 2

TASK: Define the principal actors to be included in the risk assessment process and their particular areas of responsibility with regard to the systems under consideration.

The list of actors will include the roles discussed above, technical specialists from both the ICT function and the energy supply chain functions that are relevant to the critical systems listed in the previous task, and representatives of those who will be affected by disruption to cross border energy supply.

If these actors are involved in providing input to the subsequent stages of the risk governance process then the process will be more efficient and results more useful.

Pre-assessment task 3

TASK: Define the principal documents, standards, and regulations which are pertinent to the systems being considered.

Many organisations have their own local standards and procedures, this list will include procedures and policies which are relevant at a system level, department level organisational level, Member State level, European level and international level.

The following documents, standards, and regulations have been identified by industry experts as particularly relevant to energy / ICT system interfaces.

- ISO/IEC 9000/1 - Quality Management.
- ISO/IEC 27000 series, especially 27001.2005 - Information Technology - Security Techniques - Information Security Management Systems – Requirements.
- ISO/IEC 27002.2005 (formally ISO/IEC 17799) - Information Technology - Security Techniques - Code of Practice for Information Security Management.
- ISO/IEC 27005.2008 - Information Technology -- Security Techniques -- Information Security Risk Management.
- NIST Systems Protection Profile - Industrial Control Systems V.1. 2004.
- ISO/IEC 15408 - Common Criteria for Information Technology Security Evaluation (an international standard for computer security).
- ISO/IEC 24762:2008, Information technology – Security techniques – Guidelines for information and communications technology disaster recovery services.
- IEC 61850 Communication networks and communication systems in Substations (for automation and SCADA systems).
- IEC62351 Power system management and associated data exchanges (covers security matters).
- IEC60255 Electrical relays (for protection).
- IEC60870 Telecontrol equipment and systems (General conditions, testing, communication protocols, compatibility with ISO communication standards).
- IEC60834, Teleprotection systems (General conditions, testing, communication protocols, compatibility with ISO communication standards).
- Control Objectives for Information and related Technology (COBIT) - best practices (framework) for information technology (IT) management.

- Information Technology Infrastructure Library (ITIL) - concepts and policies for managing information technology (IT) infrastructure, development and operations.

- ATEX 95 (Equipment and protective systems intended for use in potentially explosive atmospheres).

- NERC (North American Electric Reliability Corporation) good security practice.

In addition, many organisations have their own local standards and procedures that should be explicitly identified and considered in the evaluation process.

Pre-assessment task 4
Identifying possible pre-cursors to risk events is helpful as a method of early warning and helps actors to consider a wide range of possible risk events later in the process.

TASK: Consider whether changes in markets, supply chains, and technologies might have increased the risks of disruption to energy supply, in both the energy and ICT sectors.

The following list contains some of the possible areas of change identified during the study which could reveal precursors to risk events. Such changes in markets, supply chains, and technologies may increase the risks of disruption to energy supply, in both the energy and ICT sectors:

- Changes in the types of technology deployed in energy systems and ICT systems from custom designed systems to commercially available systems (COTS) e.g. the increased use of networked Internet Protocol based systems.

- Greater reliance on "standard" or commodity IT platforms, including the migration of network automation and control systems from Unix to Microsoft Windows.

- Changes to systems including renewal, modification, maintenance, decommissioning, and changes to supplier (including software and hardware changes) not accompanied by ongoing risk management, re-evaluation of business risks and appropriate security enhancement.

- Extending the connectivity of control systems and their convergence with business systems.

- Application of security standards and practices that were tailored to business systems and were not designed for previously isolated control systems.

- Increased number of access points to private and public networks, including the use of wireless networks.

- Increased integration of operational and corporate networks to support data sharing between real-time monitoring and control systems, energy trading and risk management, and other enterprise applications.

- Increased outsourcing of IT service provision, with longer chains of suppliers.

- The deployment of smart metering, sensors and other intelligent electronic devices (IEDs) on the grid.

- The increased use of new technologies for energy generation, distributed generation and smart grids.

- The increased distribution and interdependency of ICT systems.

- The increased use of remote system access for support provided by internal or external parties.
- The increased use of remote data storage accessed via private or public networks.
- Use of more IP-based communications between networks.
- Growing complexity of ICT solutions.
- Reliance on maintaining *security through obscurity,* i.e. when control systems are based on customised or antiquated software that is ostensibly impenetrable to outsiders.
- The increasing trade of cross border energy supplies in Europe.
- A lack of awareness of the seriousness of these issues amongst senior managers.
- Readily available information about control systems and their properties.
- Pressure to reduce costs.
- Pressure to implement change in a shorter timescale.
- Increased awareness amongst potential attackers of the range of threats that could be used.
- External events (political change, organisational change and personnel change).
- Increasing use of cloud computing to support business applications online with data stored on distributed individual company servers.
- Increasing pressure on shared electricity grid networks.
- Increasingly complex policy and regulatory space.

This list is used later in the process to help identify new or emerging threats to critical systems.

COMMUNICATION PROMPTS (pre-assessment phase)

- ✓ Have you recorded the list of potential critical ICT/Energy system interfaces throughout the energy supply chain?
- ✓ Have you agreed the scope and purpose of the risk governance process with your key actors?
- ✓ Have you agreed with all of the actors who are to be involved in this process what their contribution is to be?
- ✓ Have you recorded the relevant documents and standards?
- ✓ Have you involved your key actors in creating a list of pre-cursors to possible risk events?

5.4 Appraisal phase

IRGC: Combining a scientific risk assessment (of the hazard and its probability) with a systematic concern assessment (of public concerns and perceptions) to provide the knowledge base for subsequent decisions.

Appraisal task 1
This task defines the specific energy/ICT interfaces where ICT functional failure can disrupt energy supply across a boundary.

TASK: Using the list of potential target systems from the pre-assessment phase, consider the impact resulting from a functional failure of each system and score each of them according to an agreed scale.

For the European Critical Infrastructure project the following scale should be used for this task, which has been validated through workshops with industry experts. The chosen score should represent the worst that could happen if the system were to fail.

High criticality	H	Functional failure of ICT service would immediately impact energy supplies in more than one member state.
Medium-high criticality	MH	Functional failure of ICT service would impact energy supplies in more than one member state if not rectified within 24hours.
Medium criticality	M	Functional failure of ICT service would impact energy supplies in more than one member state if not rectified within 1 week.
Medium-low criticality	ML	Functional failure of ICT service would impact energy supplies in a single member state, but the cost or efficiency implications for the industry participants could be significant.
Low criticality	L	Functional failure of ICT service could impact energy supplies in a single member state, but the cost or efficiency implications for the industry participants would be minor.

Note: All of the criticality levels above ML clearly also include cost and efficiency implications for the industry participants as well. Cost or efficiency implications for the industry participants might include the staff time investigating an incident, staff time to rebuild affected ICT systems, or the costs and time associated with restoring energy supplies and/or reconfiguring energy infrastructure.

This impact score can be recorded in table 1 (Annex 5).

Appraisal task 2

TASK: Review the concern assessment for the threat of energy disruption due to critical energy/ICT interfaces.

As we stated in Section 1.1 above, the energy sector has been included as a priority sector by the EU. It is up to each Member State to designate specific ECI's. By definition therefore there would be a high degree of concern amongst the wider stakeholder community surrounding any threat to energy disruption. However, it is less likely that the level of concern would be significantly different for energy disruptions caused by the ICT interface than by any other cause (physical asset failure, bad weather, etc).

Individual Member States may opt to undertake a more detailed concern assessment for their particular local circumstances. For example, a study of the potential political, cultural or social response to energy disruption, a better understanding of the public's concerns and perceptions of energy supply, their concerns due to perceived inequalities in benefits or impact, and any ethical issues raised. It may be that there is significant resistance to energy infrastructure projects, or that there are different levels of concern in different Member States.

This is not a requirement of the framework but such research would help Member States to compare the priority of the energy/ICT interface with other critical infrastructures and therefore potentially heighten or lesson the general level of concern. This additional research may also provide valuable evidence for business cases for actions to manage risks.

Appraisal task 3
This task identifies the known or potential ICT threats through which the Energy/ICT interfaces (targets) could be compromised, and establishes the likelihood of this occurring.

TASK: For each of the potential target systems identified in task 1, list the most likely threats that could successfully compromise the system and cause failure, given the defences which are in place today.

Not all threats will be relevant to every system, because some types of threats may be eliminated by the way that individual systems are protected. The types of threat that should be considered are shown in the box, as identified through an extensive literature search and validated through workshops with industry experts. The risk pre-cursors identified in the pre-assessment phase of the process can be used to test if systems are able to cope with recent or future change. This may reveal additional threats to critical systems.

The types of defences that are typically employed are discussed in Annex 8.

Threats from system lifecycle faults

- Incorrect ICT system requirements specification, including de-specification due to budget constraints or omission of required functionality from the specification (e.g. omission of redundant systems, diverse design or emergency management for incidents such as flood and fire).
- Incorrect ICT system design (e.g. communications dependency on a mains electricity supply).
- Inadequate ICT system implementation, including meeting required service levels (e.g. caused by not providing the necessary separation of backup facilities).
- Inadequate ICT system maintenance or action if a function fails, including the risks created when suppliers of ICT services change ownership.

Threats from external system dependence

- Failure of third party ICT systems at critical times (this could be a result of many factors, from cyber threats, loss of power through to the unavailability of a service e.g. telephony as a result of normal maintenance activities).
- Lack of emergency response capability (e.g. insufficient ICT capacity to deal with a widespread disruption of energy supply caused by some other mechanism).
- Lack of disaster recovery arrangements (systems and procedures are not in place to restore services after an incident has occurred).

Threats through electronic interfaces

- Insider attack on ICT systems (an insider is an employee or any person with legitimate access to critical systems).
  - Deliberate (e.g. a disgruntled or coerced employee or IT contractor who uses their legitimate access to cause harm).
  - Accidental (e.g. who accidentally causes a disconnection, or whose intervention incorrectly overrides the correct automated system response).
  - Coerced (e.g. someone is being coerced by a 3rd party to cause harm using their legitimate access).
- External party attack on ICT systems (terrorism, hackers, thrill seekers, etc).
  - Targeted attack (e.g. an attempt to hack into a critical system to gain control of it

using either a system weakness or a stolen legitimate identify).

- Distributed attack (e.g. an attempt to overwhelm network capacity via a Denial of Service (DOS) attack).
- Non-targeted attack (e.g. existing viruses / worms / trojans / phishing / spyware weapons both in general circulation, and new weapons for the period of time it takes to create and apply a suitable defence).

The likelihood of a threat successfully compromising a system will depend on the particular combination of potential threats to each system and the defences in place as described above.

Appraisal task 4

TASK: For each system with a criticality score, identify the likelihood of a threat being successful.

For the European Critical Infrastructure project the following vulnerability scale should be used for this task, validated through workshops with industry experts and consistent with European Critical Infrastructure analysis:

Frequency of threats	multiple per day	ML	MH	H	H	H
	1 per day	L	MH	H	H	H
	1 per month	L	M	MH	H	H
	1 in next 1 year	L	ML	M	MH	H
	1 in next 10 years or fewer	L	L	ML	M	MH
		highly effective	mostly effective	possibly effective	mostly ineffective	totally ineffective
		Strength of existing defences				

The relative strength of defences can be a qualitative measure if there is sufficient evidence of the effectiveness of defences, or if this is not available, then a quantitative expert view can be used as follows.

Effectiveness of defences against types of threats:

Qualitative measure	Quantitative measure
Highly effective	Defended for over 99.999% of threats (five 9's)
Mostly effective	Defended for between 90% and 99.999% of threats
Possibly effective	Defended for between 10% and 90% of threats
Mostly ineffective	Defended for up to 10% of threats
Totally ineffective	No defences are effective for threats

It is likely that functional failure of each system could be caused by a number of different threat/defence combinations. A quick approach is to select the threat/defence combination that is most likely to cause a system failure using expert knowledge and experience, then estimate the likelihood using the suggested vulnerability scale. A more thorough approach is to use a fault tree analysis to calculate the likelihood of a range of threats being successful.

Table 1 (Annex 5) can be used to record each risk event as a combination of the vulnerability of systems to threats along with the impact of a successful threat.

To help with this task see the box that provides some hints and tips for calculating the vulnerability of systems to threats.

Hints for evaluating the vulnerability of a system to a threat

Step 1: Estimate the potential frequency of threats by either using data of the actual number of incidents per year of each threat being detected, or estimating a frequency based on the following considerations:

- The number and type of potential attackers who may exist (external party, insider staff, insider partner, inherent system flaws);
- The type of organisation that you are and whether you are more or less likely to be targeted by attackers (in this case the energy sector is a high profile industrial sector with critical infrastructure, therefore highly likely to be targeted for non-financial gain);
- The potential threats (system lifecycle faults, external system dependencies, virus and worms, web defacements, denial of service, unauthorised intrusions, physical failures, etc.).

Step 2: Consider the effectiveness of the defences in place to protect systems from these threats:

- The existence and use of security policies and processes (information security policy, data retention policy);
- System design and implementation (compliance with relevant standards such as ISO/IEC 27000-series (Information Security Management System (ISMS) family of standards), compliance with Common Criteria for security, access to data is controlled with transaction zones in place, event log monitoring in place, security patches up to date, network security testing takes place, forced password changes, spyware detection in place, network encryption deployed, virus detection deployed and up to date);
- ICT Infrastructure (private networks and systems are connected to public networks, remote access and control used, use of web applications, internet facing systems exist, wireless networks used);
- Physical access (for example theft, disposal, shoulder browsing, fire/flood/earth quake);
- Personnel (screening, security training, awareness, mock incident testing, partner facing security).

Step 3: Combine the frequency of attacks with the strength of current defences to estimate the likelihood of a successful attack (representing the vulnerability of a system to threats). This is unlikely to be able to be quantified using data, however an estimate can be made based on how many of the above threats may exist and how strong a company's defences might be using the above points as a check list.

Using a fault tree analysis a range of possible threats and defences can be combined to calculate a likelihood of a system being compromised. This approach requires knowledge about the likelihood of each individual threat / defence combination, but is likely to produce a more accurate result.

The above lists were compiled using the 'Computer Crime and Security Survey 2008 (CSI/FBI)' and the '2008 Databreach investigations report (Verizon Business Risk team)'.

A successful attack on a particular system represents a 'risk event'.

By using this systematic approach to listing systems, threats and defences, it is likely that any gaps in defences have already been identified. These are systems which if attacked, will have a high likelihood of being compromised.

It is also helpful to categorise each risk event according to the quality of knowledge available. Describing risks in this way helps to identify the appropriate actions that can be taken to explore and deal with the risk later in the risk governance process.

Appraisal task 5

TASK: Categorise each risk event according to the quality of knowledge available.

The risk event could be:

Complex: due to a complex relationship between the cause and effect of a risk event it is difficult to identify and quantify the vulnerability of a ICT/energy system. This may be because there is no strong association between a specific threat and its defences, there may be interdependencies between a range of threats and/or defences, and there may be delays between when a threat is made and when its effects are observed. Additional knowledge is needed about cause and effect chains to resolve this complexity.

Uncertain: there is uncertainty about the timing or impact of a particular threat. The threat may have different effects due to different system defences, different environments, random events, lack of knowledge. Additional evidence about the effect of threats is needed.

Ambiguous: there is a lack of agreement amongst actors about the characteristics of the threat, the effectiveness of the defences and/or the impact of the risk event. Additional engagement and discussion between actors is required.

Simple: the risk event is not characterised by any of the above situations and has a clear link between cause and effect.

Table 1 (Annex 5) can also be used to record the risk category for each risk event.

COMMUNICATION PROMPTS (appraisal phase)

- ✓ Have you confirmed that actors have a common understanding of key terms being used to describe systems and risks?
- ✓ Have you asked experts to score the impact of system functional failure for each critical system?
- ✓ Have you asked experts to list the most likely threats for each critical system and estimated their vulnerability?
- ✓ Have you confirmed that the data being used to quantify vulnerability of systems is consistent across the process?
- ✓ Have you agreed with actors the categorisation for each risk event (simple, complex, uncertain or ambiguous)?
- ✓ Have you done a concern assessment for each critical system?

5.5 Characterisation and Evaluation Phase

IRGC: In which the scientific data and a thorough understanding of societal values affected by the risk are used to evaluate the risk as acceptable, tolerable (requiring mitigation), or intolerable (unacceptable).

Using the potential impact of risk events and the vulnerability of systems, the risk events can be placed on a risk tolerability matrix. This can be used to create a consistent and clear understanding of the types of risk events which are acceptable, tolerable and unacceptable. The tolerability used in this matrix has been validated in a workshop with industry experts.

> Red: the risk is **intolerable** and requires immediate action to change the impact or likelihood of the event
> Amber: the risk is **tolerable**, some action is recommended to reduce the impact or likelihood of the event
> Green: the risk is **acceptable**, no further action required

Vulnerability					
H	🟧	🟧	🟥	🟥	🟥
MH	🟧	🟧	🟧	🟥	🟥
M	🟩	🟧	🟧	🟧	🟥
ML	🟩	🟩	🟧	🟧	🟧
L	🟩	🟩	🟩	🟧	🟧
	L	ML	M	MH	H
	Impact				

🟥	Intolerable risk
🟧	Tolerable risk
🟩	Acceptable risk

If this Risk Governance Framework is being used for risk management outside the European Commission Critical Infrastructures Programme then the tolerability of risks may be different.

Characterisation and evaluation task 1
The task reveals which risk events are important and must be dealt with.

> **TASK:** Place each risk event which has been identified on a risk tolerability matrix. Use the impact and vulnerability values recorded in previous tasks.

A suggested template for a risk matrix is attached to this guidance as table 1 (Annex 5).

Before proceeding with the final phase of the risk governance process it is worth reviewing and summarising the results of the decisions made so far. Deciding how tolerable a risk event is sometimes reveals information that was missed during the appraisal phase.

Characterisation and evaluation task 2

TASK: Review results so far to reveal any missing information or concealed risk events.

Ask the following questions:

- Have all the critical systems been identified? - look for any gaps in the supply chain analysis to check that the list of critical systems is complete. Using the table structure in Annex 7 will help to identify any gaps.

- Do you have enough quality information about the intolerable risk events to be confident in your judgment? – if any of the intolerable risk events are complex, uncertain or ambiguous perhaps some more work is required to reduce the number of unknowns before a decision should be made.

- Have any of the intolerable risk events been identified because of recent events? – review the list of pre-cursors from the pre-assessment phase, if none of the intolerable risks are a result of any of these precursors then check that defences are sufficient.

If necessary step back in the risk governance process and modify the relevant decisions.

Characterisation and evaluation task 3
At this stage of the process it is helpful to provide a summary of the decisions which have been made in prioritising risk events. This describes where management attention is required to deal with priority risks and summarizes the rationale for prioritising the risk events.

TASK: Describe the prioritised risk events, with supporting rationale.

Table 2 (Annex 5) provides a template which can be used to summarise key pieces of information about the priority risks.

The subsequent and final phase of the Risk Governance Framework deals with how best to manage these prioritised risks.

COMMUNICATION PROMPTS (characterisation and evaluation phase)

- ✓ Have you confirmed the levels of risk tolerability with key actors?
- ✓ Have you plotted the critical systems on the tolerability risk matrix?
- ✓ Have you confirmed the resulting prioritisation of critical system risks with all actors?
- ✓ Have you reviewed the process and decisions made so far with actors to check the credibility of the risk prioritisation and reveal any concealed risks?
- ✓ Have you confirmed the rationale behind each priority risk with all actors?

5.6 Management phase

Effective risk management requires the creation of a strategy, implementing the strategy through a plan of activities, and monitoring the effectiveness of the activities, so that the strategy can be reviewed and adapted if necessary.

Management task 1

> **TASK:** Consider the available options to manage the priority risks and choose which would be most effective. Form a risk management strategy.

The options for managing risks for each system will depend on the possible threats and current defences in place. The list of threats and defences for each system should be used to generate a set of options which will:

- Guarantee functional continuity of a system: to guarantee the functional continuity of a system when threatened, reducing its vulnerability. Examples include system design and implementation according to standards, the secure design of ICT infrastructure, protection from physical threats and security awareness training for personnel.

- Reduce the impact of a system failure. Examples include early warning services, redundancy for systems, networks and power supply.

- Reduce the time taken to recover from a system failure. Examples include preparedness plans, incident management governance arrangements in place, training for emergency response, restoration of systems from backups and security and data retention policies.

Annex 8 provides a list of example defences, which can be deployed to reduce the risks of a successful threat.

Each risk event has also been categorised as a simple, complex, uncertain or ambiguous risk event. This categorisation can help identify the sort of options that should be considered.

Simple risk problems: Risks can be reduced by applying existing standards or good practice.

Complex risk problems: Additional expert study is needed to get a complete and balanced set of risk and concern assessment results. This will provide greater confidence in the knowledge about a risk event and therefore confidence in decisions about tolerability. The knowledge will also help to choose the right risk management options to reduce the risk.

Risk problems with uncertainty: Unresolved uncertainty implies that the characteristics of the risk are not (yet) known, one should adopt a precautionary based strategy so that irreversible decisions are avoided. Experts and directly affected stakeholders should be asked about uncertainty. Small risk management steps are required so that the management process can be stopped or even reversed as new knowledge is produced or negative side effects become visible.

Risk problems which are ambiguous: If risk assessment results are interpreted differently by different actors (including the public) and if there is controversy over what should be done, then management needs to address the causes for these conflicting views and seek resolution before deciding on the actions required to reduce the risk.

Once a set of options has been created for each priority risk event, they should be evaluated in order to choose the most effective options.

For each option evaluate:

- Is it effective?
- Is it cost efficient?
- Does it have any unintended outcomes?
- Is it a sustainable option?
- Is it a fair option for all parties concerned?
- Is it legal and politically acceptable?
- Is it ethical?
- Would it have public support?

Choose a combination of options which provide confidence that the risk will be reduced. Identify a target tolerability score which is expected to be achieved by implementing these options. The new score will be based on the reduction in vulnerability of the system and/or reduction in impact of the risk event.

Table 2 (Annex 5) can be used to record these decisions.

The next stage is to plan who should implement these options, by when, and gain their commitment to this risk management plan.

Management task 2

TASK: Plan who should implement activities to manage risks, by when, and gain their commitment.

A senior director or senior manager should sponsor a risk management plan give it the necessary authority within the organisation. Where actions are required in more than one organisation, particularly in more than one country, there should be an equivalent level of sponsorship in each organisation involved. The plan should contain activities, objectives and milestones which implement the risk management options chosen in the previous task.

It is unlikely that there will be direct equivalence between the roles and responsibilities of actors in different organisations, Member States, or other countries. Any lack of equivalence should be recognised and managed by the actors involved to ensure a common understanding of the outputs which are required. This may require changes to existing policies and procedures, or even changes to bi-lateral or multi-lateral agreements between organisations in different Member States.

A risk manager would normally track the progress of agreed risk management actions that arise, and confirm with all actors involved in the activities that they understand and accept their responsibility and accountability.

Table 2 (Annex 5) can be used to record agreement of the actions and responsibilities of the actors involved.

The next task is to monitor the implementation of the risk management plan.

Management task 3

TASK: Evaluate progress of risk management and if necessary improve the programme.

It is important to choose indicators which provide a good representation of progress, normally a combination of the progress of key activities (e.g. updating and testing a policy, training of staff, provision of encryption for remote office workers) and the delivery of outcomes (a reduction in the risk appraisal scores).

Progress against these indicators would be measured at intervals and compared with expected progress. If progress is below expectation then the effectiveness of activities should be reviewed. Alternatives activities from task 1 can be considered which may prove more effective at reducing risks.

It is important that the decisions taken in this Risk Governance Framework should also be reviewed in light of any changes to ICT systems or energy infrastructure. The list of risk pre-cursors provides a useful prompt to consider the importance of any recent events.

COMMUNICATION PROMPTS (management phase)

- ✓ Have you received ideas for potential risk management options from all stakeholders?
- ✓ Have you involved the relevant expert actors in the evaluation of each option?
- ✓ Have you agreed the best combination of options with key actors?
- ✓ Have you agreed the responsibility and accountability for risk management actions with relevant actors (including from other organisations / other member states)?
- ✓ Have you agreed the objectives and milestones for each action with relevant actors?
- ✓ Have you agreed the indicators for measuring progress with relevant actors?
- ✓ Have you summarised the whole risk management plan and sent it to all of the actors involved in the process?

5.7 Outputs

The following outputs result from using this Risk Governance Framework.

Prioritised list of risks considered

- A list of all risks, in prioritised order from high risk to low risk.

Outcome: A clear understanding of which risk events are important and must be dealt with.

Evidence for an individual risk assessment

A detailed description of a selected risk event;

- Which target is at risk from which threat(s),
- The impact of a successful attack and,
- The likelihood of an attack being successful.
- The resulting tolerability of the risk.

Outcome: A clear description of the evidence supporting a risk priority.

Priority risks for attention

- The priority risk(s) with an explanation as to why the risk(s) is high priority (its tolerability score in terms of impact and likelihood).
- A clear understanding of the priority of the energy/ICT interface as a critical infrastructure in comparison with other Member State critical infrastructures.
- Evidence for business cases to take steps to manage risks.

Outcome: A clear understanding of where to focus management effort to reduce risks.

Risk management strategy

- An action plan for how the high priority risks will be tackled, by when, who is responsible, and how progress and successful completion of the action plan will be measured.

Outcome: A clear plan of action to reduce the priority risks, with accountable actors and deadlines, potentially involving actions that need to be taken on a bi-lateral or multi-lateral basis between Member States.

6 Conclusions and Recommendations

6.1 Conclusions

The suitability of the risk governance framework developed

- The Risk Governance Framework elaborated under this project draws heavily on a model developed by the International Risk Governance Council. The IRGC risk governance framework considers the complex interdependencies between stakeholders and between systems, therefore is well suited for this subject area. The IRGC model has been modified to suit the purpose of identifying and managing ICT related risks faced by EU critical energy infrastructures.

- The Risk Governance Framework does not replace but encompasses relevant existing detailed technical and risk management standards and procedures (which should be agreed upon in the pre-assessment phase by the stakeholders involved) such as ISO 27001 and 27005, UCTE operational security handbook and security operations. The purpose of the risk governance is to engage all relevant stakeholders in the decision making processes to ensure risks are appropriately identified and managed.

- The current banking crisis has highlighted the need for appropriate national and regional government organisations to be reassured that organisations operating and regulating key national and regional infrastructures have adequate risk governance processes in place, not only to protect their own business continuity, but also to protect the wider communities.

Key conclusions arising from the questionnaire and stakeholder workshops

- There was general agreement that the framework will be useful for its defined purpose (to identify cross-border risks, to encourage good practice, to ensure a consistent approach, to identify types of risks).

Key conclusions arising from the stakeholder workshops

- Stakeholders raised concern about the any additional resource requirements to apply a Risk Governance Framework.

- Different people use different terminology and in particular energy technologists do not use the same language as ICT experts. In practice, this is not a problem since the terms can be clearly defined during the risk governance process so that a common understanding is achieved.

Key conclusions arising from the questionnaire responses

- There was general agreement that the framework will help consistently apply best practice, identify and quantify risks, and provide clarity in assigning responsibilities.

- However, there were mixed views (disagreement 6/14, agreement 8/14) that the Risk Governance Framework can provide a high level interface with existing national risk governance arrangements for communicating results with the Commission and other Member States.

- And there were mixed views (disagreement 4/15, agreement 11/15) that the Risk Governance Framework will provide a concise summary of the types of defences that might exist.

- Functional failure of the following ICT-energy interfaces are expected to have the highest impact (note: high impact does not necessarily result in the highest risk if an impact is unlikely):

    - Electricity sector: Transmission systems (remote control, SCADA systems and safety systems), real time generation and dispatch (remote control and SCADA systems).
    - In addition, the sister Study on Critical Dependencies of Energy, Finance and Transport Infrastructures on ICT Infrastructure identified messaging services and file transfer service for the electricity sector and, for the gas sector, identified compressor stations, control centres, pressure control systems and export stations (containing compressors and mixers) as potentially most critical. Communication systems such as private LAN and WAN networks were identified as critical for both electricity and gas.

- Some organisations have defined procedures for a risk governance process and processes for assessing the risks and dealing with them – however most organisations use ‘ad hoc methods without formal guidance’.

- The majority of stakeholders verified the use of the ISO standards for ICT including requirements, code of practice, and risk management (ISO/IEC:27000 series).

Key conclusions arising from the literature review

- The literature review highlighted the fact that information security professionals are seldom involved in the design, planning, implementation and management of ICT systems for the energy sector. In some cases, the security of ICT and energy systems will be handled by separate departments where personnel may use different terminology. The Risk Governance Framework should be applied jointly by IT and energy departments. The Risk Governance Framework will need to cut across different actors, different languages, disconnects and consider interdependencies. Establishment of a Risk Governance Framework will flush out intradepartmental language/communication problems (especially in relation to IT terminology).

- There is a potential for ICT failures to cascade into the energy sector and through into other critical sectors. The dependence on information systems introduces security issues that can have a significant impact on the resilience and reliability of critical infrastructures, regardless of whether the supporting systems are centralised, standalone or embedded.

- The vulnerability of computer networks does not necessarily entail the equal vulnerability of the critical infrastructures these networks support. In many cases redundancy is built into energy systems. This echoes with the findings of the sister Study on Critical Dependencies of Energy, Finance and Transport Infrastructures on ICT Infrastructure.

- However, as the use of ICT to control energy systems and respond to crises grows and becomes more reliant on commercial off-the-shelf IT technologies, vulnerabilities will increase.

- The project identified a range of areas of change in markets, supply chains, business processes and technologies which could constitute precursors to risk events by increasing the risks of disruption to energy supply, in both the energy and ICT sectors. In line with this finding, the sister Study on Critical Dependencies of Energy, Finance and Transport Infrastructures on ICT Infrastructure found that all sectors invest heavily in build-up and operation of redundant ICT systems. However protection or mitigation capability is weak with regard to “new” ICT-threats despite the fact that sophisticated degradation modes are available to mitigate such vulnerabilities.

Key conclusions of relevance arising from the sister project European Network of SCADA Security Test Centres for Critical Energy Infrastructures

- A Risk Governance Framework will be useful to Member States so that they can confidently define the possible attack/threat scenarios, which in turn can be considered by a SCADA test centre to ensure that tests are comprehensive.

- Any system or component vulnerabilities which have been identified by tests must be treated with utmost confidence (risk of falling into the wrong hands). This finding is of particular relevance when considering how completed Risk Governance Frameworks can be shared with relevant parties without compromising security.

- A whole system life cycle approach to security is required and security training at all stages of a system’s lifecycle is required.

- Security needs to be embedded within the organisation’s governance and behaviour, not as an add-on. It is a costly exercise to design and test for security, this needs senior level support. This finding echoes findings from the stakeholder consultation on the proposed Risk Governance Framework.

Key conclusions of relevance arising from the Critical Infrastructure Protection Expert Group

- Member States are developing their own systems for identifying and managing risks at organisational and national levels (eg. Sweden’s interactive tool for dependency analysis). The group also indicated that it would be useful for EU to have a practical tool for identifying these best practices and ensuring that EU critical infrastructures are properly assessed. The Risk Governance Framework aims to meet this need with regard to ICT-energy infrastructures. There is potential to develop a similar tool for other sectors.

6.2 Recommendations and next steps

Applying the framework – who

- Member States should be free to select the most appropriate organisations to be involved in applying the Risk Governance Framework.

- It is recommended that neighbouring or interdependent countries carry out joint assessments as they see fit. Member States at the end of supply routes may be more interested in using the Risk Governance Framework (to identify risks from further up the supply chain) than those at the middle or at the beginning of the energy supply chain. Commercial confidentiality concerns may also limit information sharing.

- Organisations may find the Risk Governance Framework useful where no standard procedures and policies are in place to assess and manage risks, or where such procedures and policies do not consider cross border risks.

- Individuals applying the Risk Governance Framework need to be trained centrally to ensure consistent outcomes. Existing risk experts from Member States could be trained to take on this role.

Applying the framework - the role of the European Commission

- The European Commission as a supra-national actor would theoretically be in the best position to apply the Risk Governance Framework together with Member State authorities, companies, stakeholders. However stakeholders have expressed concern in reporting to the Commission on their risk management procedures.

- However, the results of applying the Risk Governance Framework do not necessarily need to be submitted to the EU, as long as the Commission have assurance that organisations are assessing and managing cross border risks. In this respect, the Risk Governance Framework could be used as the basis for an audit of energy infrastructure companies, on behalf the European Commission. Cross-over with current reporting required under Directive 2008/114/EC[20] should however be considered.

- The European Commission may be able to provide financial support to strengthen points in the system identified as weak.

Applying the framework – when

- The literature review indicated that the subject of ICT threats and defences with regard to CIP is a developing field, with new cyber attacks being created, and there are increasing numbers of interdependencies between ICT systems in energy supply, e.g. smart grids. There is an expectation that these ‘risk precursors’ will increase the vulnerability of cross border energy supply to risks, which need to be recognised and managed appropriately. There is therefore a sense of urgency to apply this framework, and review it.

[20] Directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection.

- The frequency with which a risk assessment is done should be determined by:
  - the outcomes of the first assessment,
  - by regular assessments of risk precursors looking for significant changes, and
  - in line with other key milestones in the EPCIP.

Applying the framework – how

- A structured implementation plan is required. The Risk Governance Framework allows Member States specific situations to be incorporated whilst retaining a common framework under which cross border ICT-energy risks can be identified.

- Before applying the framework, users should review the language used in the Risk Governance Framework to ensure both energy and ICT professionals have a common understanding.

- The framework can be applied at all levels of resolution, but will demand more time and effort if detailed technical procedures are reviewed as part of the exercise. It is recommended that those applying the framework are assisted by qualified individuals who can ensure a consistent approach is followed. Existing risk experts from Member States could be trained to take on this role.

Implementing the framework into EU legislation

- The Risk Governance Framework should be consistent with other actions in the EPCIP and should be informed by other ongoing EPCIP activities and projects.

Raising awareness, validation and equipping Member States

- There is good support for the need for the Risk Governance Framework, but there was limited support provided during the project to critique and validate the framework. Further validation would provide greater confidence that the principles used in this framework have wide stakeholder support.

- In order to raise awareness of the Risk Governance Framework and its uses, and to gain Member State support, the Commission may consider carrying out a series of Member State/regional roadshows for relevant experts and officials, also covering other EC initiated ICT CIP activities.

- To demonstrate / pilot the Risk Governance Framework to key stakeholders, train potential MS users in the application of the Risk Governance Framework and to further validate the RGF, we propose the following programme of workshops:

  - A workshop with the EPCIP expert group, in collaboration with ENISA to demonstrate the Risk Governance Framework (the rationale, approach, worked examples);

  - A workshop with Energy / ICT experts to demonstrate the application of the Risk Governance Framework (the rationale, approach, fictitious case studies to work through, training in the application of the Risk Governance Framework);
  - A full day or 2 day workshop with targeted experts using real world situation(s)
    - It is recommended that real data and information is collected in advance from participating member states – although this would be time consuming and data sensitivities would have to be addressed, this approach is likely to deliver more value for the Commission and participating Member States as it would identify any vulnerabilities to specific cross border energy supplies.
    - Fictitious scenarios would be easier and quicker to prepare and although they would not identify any real vulnerabilities, this would provide additional confidence in the Risk Governance Framework process and templates.

Further improvement or extension of the Risk Governance Framework

- Concern assessment: The project focussed on the risks to disruption to cross-border energy supplies, with an assumption that this was of significant concern. However, Member States may wish to carry out additional research to review this predefined ‘concern assessment’, looking at the economic impacts (to organisations and governments) of interruptions to cross-border energy supplies, and any wider societal concerns. If this research were to be carried out at an EU level then a consistent EU wide ‘concern assessment’ review will ensure results of any risk assessments are consistent between Member States. However, this is likely to be a very difficult and complex piece of research, and may not be acceptable by different Member States. To illustrate this, our energy choices are influenced by societal discussions that have the potential to conflict with technical risk assessment results (e.g. about the safest mode of delivering energy etc). Furthermore, the results of a concern assessment will vary in different countries (e.g. French and German citizens do not have the same risk perceptions about nuclear energy because the French put more trust in their regulatory system, so that nuclear power is more accepted in France than in Germany). However, investigating these differences of perception and examining where there are similarities and differences enables the initiation of a dialogue which may result in a better common understanding of the real and perceived risks.
- Application to other sectors and critical infrastructures: The Risk Governance Framework process can be used for other situations (with appropriate modifications to the impact scale), to identify vulnerabilities to cross border or cross boundary services:

  - ICT threats to the transport sector;
  - ICT threats to the finance sector;
  - ICT threats to energy supply / transport / finance between organisations;
  - ICT threats to energy supply / transport / finance within Member States borders.

- Publication: The Risk Governance Framework needs to be translated into various media for publication, with templates, a handbook, web site and training materials (derived from the content of the report) for potential Member State practitioners. The report, templates and guidelines constitute the basis for a training programme.

- Sustainability: Due to the emergence of new cyber threats and their associated defence mechanisms, and the increased interdependence of ICT systems and use of new technologies, the Risk Governance Framework materials must be reviewed and kept up to date (living documents owned by established working groups) e.g. lists of potential threats, lists of possible precursors, refine scales, and develop worked examples.

7 Glossary

Term	Definition
CIWIN	Critical Infrastructure Warning Information Network.
Data logging and metering	Data not available in real-time.
Denial of Service (DOS)	A class of network security threat whereby one or more attackers target computer systems, network resources and servers to make them inaccessible by denying service to legitimate users. [Cs3 Inc.; U.S Secret Service/Carnegie Mellon University 2005].
DCS	Digital Control System.
Hazard	A source of potential harm or a situation with the potential to causes loss. Source: IRGC (2005).
High Criticality	Functional failure of ICT service would immediately impact energy supplies in more than one MS.
Information Communication Technology (ICT)	Electronic information-processing technologies such as computers and the Internet, as well as fixed-line telecommunications, mobile phones and other wireless communications, networks, broadband, and various specialised application devices ranging from barcode scanners and Braille readers to global positioning systems (GPS). Source: Digital Strategy, 2009.
Internet	Publicly accessible communications route.
Low Criticality	Functional failure of ICT service would not impact energy supplies in more than one MS. Alternative systems available to provide the disrupted functionality.
Medium Criticality	Functional failure of ICT service would impact energy supplies in more than one MS if not rectified within 1 week.
Medium-High Criticality	Functional failure of ICT service would impact energy supplies in more than one MS if not rectified within 24hours.
Medium-Low Criticality	Functional failure of ICT service would not impact energy supplies in more than one MS, but might have significant cost or efficiency implications for the industry participants.
MS	Member State of the European Union.
Pre-assessment	Identification of the breadth of issues that stakeholders and society may associate with a certain risk as well as existing indicators, routines, and conventions that may prematurely narrow down, or act as a filter for, what is going to be addressed as risk. Source: IRGC (2005).
Private leased systems	Systems granted by private entities (providers) for use during a specified contractual period in exchange for a specified payment.
Public systems	Systems routed through the public domain as part of the open market. Such systems are more prone to a failure during power system events, common mode interference, disruption, delays and sudden changes of time delays and characteristics.
Remote control	Control from an off-site location, i.e. an intervening network is used to link a control centre to a SCADA system - requires human intervention to carry out control functions.

Term	Definition
Risk Appraisal	The process of bringing together all knowledge elements necessary for risk characterisation, evaluation and management. This includes not just the results of (scientific) risk assessment but also information about risk perceptions and economic and social implications of the risk consequences. Source: IRGC (2005).
Risk Governance	Includes the totality of actors, rules, conventions, processes, and mechanisms concerned with how relevant risk information is collected, analysed and communicated and management decisions are taken. Encompassing the combined risk-relevant decisions and actions of both governmental and private actors, risk governance is of particular importance in, but not restricted to, situations where there is no single authority to take a binding risk management decision but where instead the nature of the risk requires the collaboration and co-ordination between a range of different stakeholders. Risk governance however not only includes a multifaceted, multifactor risk process but also calls for the consideration of contextual factors such as institutional arrangements (e.g. the regulatory and legal framework that determines the relationship, roles and responsibilities of the actors and co-ordination mechanisms such as markets, incentives or self-imposed norms) and political culture including different perceptions of risk. Source: IRGC (2005).
Risk Management	The creation and evaluation of options for initiating or changing human activities or (natural and artificial) structures with the objective of increasing the net benefit to human society and preventing harm to humans and what they value; and the implementation of chosen options and the monitoring of their effectiveness. Source: IRGC (2005).
Safety real time high speed protection systems	Systems that provide continuous and uninterrupted real time high speed inter-substation telecommunications and signals including data streams. Protection systems are designed with power supplies, duplications and redundancy to minimise the probability of a failure or close down.
SCADA	Supervisory Control and Data Acquisition system - the on-site control system which can continue to operate in isolation if any remote site control is lost. Carries out control functions automatically.
Third country	A country outside the European Union.
Tolerability & Acceptability Judgement	Risks are deemed to be acceptable if they are insignificant and adequately controlled. There is no pressure to reduce acceptable risks further, unless cost effective measures become available. In many ways, acceptable risks are equivalent to those everyday risks which people accept in their lives and take little action to avoid. Source: IRGC (2005).
TSO	Transmission System Operator.
	Electricity sector value chain
Fuel purchase and supply	Coal, gas, oil, uranium, renewables and onsite storage capacity.
Centralised generation providing main and ancillary services	Large scale power generation linked to the high voltage transmission network.
Embedded and intermittent generation	Small scale power generation linked to the lower voltage distribution network.

Term	Definition
Real time system balancing and generation dispatch	Real time balancing of electricity demand by Grid companies, coordinated by UCTE for continental Europe Bidding / despatching processes.
Transmission	Passage through sub-stations. Additional within country and between country interconnectors.
Distribution	Passage through Grid Transformers and Substations into and from Distribution Systems.
End users – providing ancillary balancing services	Subtransmission customers industrial, commercial and domestic users may have interruptible supplies.
End users – Critical services to ICT Sector	Banks, ICT providers etc.
End users – Critical services to other energy sectors	Power generators requiring electricity to start generating.
Energy metering and financial settlement	Means to measure and charge for energy services.
Energy trading	Systems used to trade energy commodities.
	Gas sector value chain
Primary production and supply (gas liquefaction plant for LNG)	Extraction, local processing (gas liquefaction plant for LNG) and transportation.
Import to EU and supply - Pipelines and ports	Pipelines and ports.
Storage	LNG + line pack (compressed storage in gas pipelines) + strategic stocks eg in old reservoirs.
LNG - regassification	LNG regassification infrastructure.
Processing	Pressurisation.
Distribution	Dedicated pipelines to power plants and major industrial users general industrial and commercial customers domestic users.
End users – power plants	Interruptible supplies.
End users - major industrial	Interruptible supplies.
End users - all others	Small industrial, commercial and domestic.
Energy metering and financial settlement	Means to measure and charge for energy services.
Energy trading	Systems used to trade energy commodities.
	Oil sector value chain
Primary production	Extraction, local processing and transportation.

Term	Definition
and supply	
Import to EU and supply - Pipelines and ports	Pipelines and ports.
Storage - crude	Storage of unrefined oil.
Processing	Refining.
Storage - product	Storage of refined produce.
Distribution - pipeline	Dedicated pipelines to power plants and major industrial users general industrial and commercial customers domestic users.
End users – power plants	Interruptible supplies.
End users - major industrial	Interruptible supplies.
End users - all others	Small industrial, commercial and domestic.
Energy metering and financial settlement	Means to measure and charge for energy services.
Energy trading	Systems used to trade energy commodities.

Annexes

AEA
Gemini Building
Harwell
Didcot
Oxfordshire
OX11 0QJ

Tel: 0870 190 8435
Fax: 0870 190 6318

AEA