16010846D004

UK Smart Grid Cyber Security

London, June 25th 2011

Author(s) Marc Tritschler, William Mackay

Report produced on behalf of:

Energy Networks Association
6th Floor Dean Bradley House
52 Horseferry Road
London
SW1P 2AF

author :	Marc Tritschler, William Mackay	reviewed :	Hans Pille
	81 pages 10 appendices MT, WM	approved :	Hans Pille

CONTENTS

1 EXECUTIVE SUMMARY

This report provides an approach and management framework to address the cyber security challenges faced nationally and by the Distribution Network Organisations as the current network infrastructure is developed with new Smart Grid systems and technologies. It is intended to provide a sound basis upon which detailed and enduring smart grid cyber security efforts can be built through the „low carbon transition". Two levels are considered: firstly at national level to provide an overarching approach to smart grid cyber security, and secondly at DNO level to support the development of management systems for smart grid cyber security.

The approach reviews current UK activities, European activities, several international standards and current guidelines for smart grid cyber security, essentially to gain an understanding of the current cyber security initiatives worldwide, and to understand the applicability of these initiatives in the UK. Key stakeholders were engaged to understand how cyber security is currently being addressed by the electricity network companies in the UK, and how this can be best addressed using the findings from this report. This includes national and regional considerations.

National Level:

- Cyber security should be considered from a collaborative national perspective industry wide.
- Establish, develop and maintain a national level risk assessment process for smart grids to manage, inform and drive UK smart grid activities.
- Include smart grid cyber security as part of evaluation criteria for LCNF projects.
- Incorporate smart grid cyber security considerations into the work of the Smart Grids Forum.

DNO Level:

- Develop an Operational Security Management System to bring cyber security under the explicit control of management.
- Consider risk assessment approaches and determine if appropriate for smart grid cyber security.
- Consider a Technology Change Management strategy to address cyber security.

- Consider a detailed audit programme of candidate DNOs to establish gaps in current practices and develop applicable operational security management system requirements, policies and controls to address cyber security.

2 INTRODUCTION

This introductory section is an extension of the executive summary which provides further background material and a brief overview of the main body and key points of the report, describing key considerations and initiatives required to develop and implement a structured framework to address Smart Grid Cyber Security in the UK. The main body and detail of the topics and findings are described in the Appendices of this document and referenced from the respective sections.

2.1 Background

The background section of this report considers the current network structure and highlights the features of a Smart Grid implementation. It outlines how the current network systems will be affected as Smart Grid is developed and comments on how Cyber Security must be considered when developing the Smart Grid architecture, technologies and management systems.

Key Points:

- There will be a dramatic increase in the distributed nature and complexity of network monitoring and control systems as Smart Grid is developed. This requires organisational adjustments, development of people, process and technologies.
- Smart Grid will be exposed to a dynamic threat model where threats are constantly changing and unpredictable.
- Organisational and Technical Risks should be formally managed frequently on an on-going basis at national and regional level.
- ICT security, along with computing system reliability, safety and maintainability are critical attributes for smart grid implementation and operation, and need to be considered as part of overall risk management for this Critical National Infrastructure.
- Smart metering should be considered a key component of smart grid architecture, facilitating secure participation of the domestic, industrial and commercial consumer.

APPENDIX A - Background, describes further detail of Smart Grid Monitoring and Control, Smart Metering as an element of smart grid, Critical National Infrastructure, Smart Grid Cyber Security and the Current status of UK initiatives on smart Grid.

2.2 Approach

This section makes some comment on current network architecture and the management responsibilities of various functions within the organisations with regard to cyber security. For example the current architecture has evolved to be fragmented in structure and the management around this naturally aligns to suit.

Key Points:

- Cyber security management approaches for the current electricity network architecture have a tendency to be somewhat fragmented, with responsibility for cyber security and any associated management systems split across different parts of the electricity networks companies.
- Functions within the organisations currently operate efficiently to meet regulatory requirements and guidelines, sometimes in isolation to other business functions.
- An integrated approach to managing cyber security is required where interdepartmental boundaries can be redefined along with ownership and accountability.
- Cyber Security roles and responsibilities should be defined throughout all levels of the organisation.
- Develop a high-level approach to address smart grid cyber security for the UK, including a framework for risk assessment.

The main body and detail of the findings in this section are described in APPENDIX B - Approach.

2.3 Current UK Activities

This section outlines the current UK activities which have some bearing on smart grid cyber security. It also covers government policy, regulatory environment, and current programmes of work, including the Low Carbon Network Funding (LCNF).

Key Points:

- Cyber security is currently perceived to be a sub-project of other initiatives, for example in some cases it is seen solely as a technical issue. However, there is a strong dependency between smart grid cyber security and security of supply. This involves people, process and technologies, all of which should be considered in Smart Grid development.
- The overarching objective of LCNF projects is to trial solutions which can provide security of supply in a low carbon economy; however, smart grid cyber security requirements are not included explicitly as part of these projects.
- Smart grid cyber security should be a significant consideration for the Smart Grids Forum. Also benefit would be gained by intergroup engagement with the Smart Meter Technical Experts Group (STEG) and the Privacy and Security Advisory Group (PSAG). Objective - to share and contribute security knowledge between these groups.
- Engagement with CPNI would be beneficial to help develop and encourage smart grid cyber security management practices and help develop and reposition assessment methods.
- CPNI's Good Practice Guides appear to be well utilised at operational management levels and below in industry, however, there are indications that the level of executive support is limited.
- The use of IS1 as the method of risk assessment for the SMIP has been widely welcomed, and a similar approach for smart grid risk assessment should be considered.
- Each DNO responsible for deploying its own smart grid solutions, including communications infrastructure, to its own specifications. Therefore there is a greater challenge to the coordination of smart grid cyber security efforts. This should be reviewed to establish common objectives and deploy best practice across the board where possible.

The main body and detail of the findings in this section are described in APPENDIX C - Current UK Activities.

2.4 Electricity Network Company Activities

This section provides an overview of current DNO approaches to managing cyber security including; Current Operational Network Management Systems and Processes, Governance Arrangements, Risk Management, Awareness and Training, Security Requirements and Innovation and Pilot/Demonstration Projects for Smart Grid Systems and Processes.

Key Points:

- Governance arrangements are generally well established and robust for systems which are typically identified as IT systems (including communications), this is less evident for remote equipment, including substation installed Remote Terminal Units (RTUs) and also other automation equipment and devices located both inside substations and also as stand-alone network equipment.
- A key observation in this area is that if equipment is not considered to be IT or SCADA equipment, then it will not be governed in accordance with IT or SCADA best practices.
- Laptops, programming software on the laptops, and the programmes which are being altered in field equipment are often governed only by the field engineers undertaking the work.
- Remote equipment provides potential entry points to the networks and systems upstream. Poor governance in this area can lead to opportunity for intentional network disruption.
- Typical ownership and management of operational network management systems are often split across various parts of the DNOs businesses.
- Currently there is no single role which is responsible for cyber security across all elements of the operational network management systems. This should be considered as part of a cyber security roles and responsibilities review across the organisation.
- Cyber security concerns on innovation projects appear to be focused mainly on ensuring that technical solutions are applied, particularly to communications architectures.
- Longer term governance and cyber security management on innovation projects is evidently less of a concern but should be considered as an essential requirement.
- The DNOs typically have very well established enterprise risk management approaches, enshrined in corporate policy. These are supported by risk management procedures which coordinate and consolidate risk assessment activities, providing a regularly updated corporate picture of risk across the enterprise.

- In general, physical, environmental and safety risks are adequately covered within operations and IT addresses the familiar risks of for example, of availability and performance.
- Cyber security risk assessment for operational network management systems is an intersection of the scope of operational risk assessment and IT risk assessment. This intersection is recognised informally but not recognised at enterprise level as a key area for collaborative risk management efforts.
- Awareness and training concerning operational network management systems cyber security does not appear to be well covered across the DNOs, in particular for field personnel. Generic elements such as IT security are well covered, but specific training concerning operational network management systems cyber security is not.
- DNOs are keenly aware of the need to include security requirements in specifications, in particular for new systems such as SCADA/DMS, but less so for field based equipment.

The main body and detail of the findings in this section are described in APPENDIX D - Electricity Network Company Activities

2.5 National Grid

This section provides an overview of the role and function of the National Grid Digital Risk and Security Consulting Group.

Key Points:

- The objective is to protect key operational assets.
- Provide security related input to project and organisational initiatives.
- Engage in security risk and business impact assessments.
- Global pool of knowledge and resource.
- Manage outsourcing with partners.

The main body and detail of the findings in this section are described in APPENDIX E – National Grid.

2.6 European Activities

This section describes European level activities with relevance to smart grid cyber security, focusing both on European Commission sponsored activities and directives;

Key Points:

- The scope of the activities and recommendations of the European Smart Grids Task Force Expert Group 2 are focused mainly on tackling issues such as energy theft and privacy.
- Expert Group 2 does not consider smart grid cyber security from the perspective of smart grids being part of the CNI.

The main body and detail of the findings in this section are described in APPENDIX F - European Activities.

2.7 International Standards and Guidelines for Smart Grid Cyber Security

This section provides an overview of wider international standards and guidelines including NISTIR 7628, ISO/IEC, ANSI standards and CPNI Guidelines, specifically to establish their applicability to provide a framework for Cyber security in the UK.

Key Findings

- NISTIR 7628: In some literature and by some in the cyber security community NISTIR 7628 is loosely referred to as a „Standard" which in itself may imply an association with some level of regulatory compliance. This is not the case or intention of 7628, they are Guidelines best used selectively to assist in the development of low level cyber security requirements. The material within the volumes is more aligned to a bottom up approach.
- ISA99.02.01-2009: This is a standard for "Security for Industrial Automation and Control and is now approved and published by the IEC as 62443-2-1 (November 2010). There is a current on-going development to adjust this standard to align more closely with the ISO/IEC 27000 family of standards and ISA have committed to completing this work by the end of 2012. A new version is expected to be complete by the end of 2011
- ISO/IEC 27001/27002: This standard and code of practice (27002) are based on risk management and formally specify an information security management system which brings information security under the explicit management control. This is a strong

candidate which can be complimented by the CPNI Guidelines as a starting point for developing a cyber security management system framework appropriate for the UK.
- Standards and guidelines employed must accommodate and align with the organisation's top level cyber security policy requirements.

The main body and detail of the findings in this section are described in APPENDIX G - International Standards and Guidelines for Smart Grid Cyber Security.

2.8 National Level Smart Grid Cyber Security Framework

This section describes a potential approach for a national level smart grid cyber security approach, including risk assessment, and the completion of initial steps to help quantify the scope and scale of smart grid risk assessment efforts;

Key Points:

- An overall smart grid risk assessment at national level will help develop an understanding of the prospective scope of smart grids, and will assess security risks at this high level. The results of this approach could then drive further more detailed activities at DNO level.
- Completing and subsequently maintaining a smart grids risk assessment at national level using IS1 as a basis would allow DECC to develop and maintain an overview of the key smart grids risks, which could then be used to drive/steer DNO security related activities.
- It should be noted that the IS1 standard is focused on technical risk assessment, meaning that it excludes non-technical risks such as physical risks and natural disasters.
- The work already completed on smart metering risk assessment using IS1 could provide valuable input to any smart grids risk assessment work.
- Risk assessment activity could be completed in consultation with CPNI and CESG, as has been done with the smart metering risk assessment.
- DNO"s should also be expected to identify and manage risks in their own situations and also seek to address those risks with an appropriate cyber security risk assessment process. A common and consistent risk assessment approach could be recommended across DNO"s.

- Risks associated with Security in design, installation, management and maintenance of devices in the field should be given more attention as in the future these will be smart grid devices.
- Security governance of current operational systems end-to-end needs to be considered (i.e., from control centre to the end measurement or control points on the network).
- DNOs are highly dependent on third party suppliers and service providers and third party risks are not always considered from end-to-end within current operational systems. This should be addressed as smart grids are developed.
- The Smart Grids Forum should incorporate consideration of smart grid cyber security into its work and investigate is how to deliver coordinated smart grid cyber security efforts across all stakeholders.
- The DNOs approaches to smart grid cyber security on LCNF project bids should be considered as part of the evaluation process, explicitly examining how the DNOs plan to deliver continued security of supply should the new smart grid technologies being trialled suffer cyber security vulnerabilities at any point in their lifecycle after deployment.
- The CPNI should review its good practice guides and self-assessment approach with particular focus on requirements for smart grid cyber security.

The main body and detail of the findings in this section are described in APPENDIX H - National Level Smart Grid Cyber Security Framework.

2.9 Organisation Level Smart grid Cyber Security Framework

This section details a proposed framework example for consideration by the DNOs to ensure that smart grid cyber security is appropriately supported and integrated into projects and operational activities. Currently there is no end to end overarching framework in place.

Key Points:

- Adoption by the DNOs of a structured approach such as the framework presented in this section would enable a more consistent and managed approach towards smart grid cyber security, whether as part of new technology pilots or full deployment of smart grid solutions. An operational management framework to manage smart grid end to end cyber security through development and continuous change is essential.

This should be supported and defined through a cyber security policy, driven and enforced by top management,

- The Structure of the framework, for management system purposes, is broadly aligned with ISO 27001 requirements and depicts some of the elements that should be considered by DNOs
- Accountability for cyber security will require a more integrated cross functional co-operative and collaborative approach across the organisation including third parties.
- Cyber security should be considered as an inclusive and integrated element of job function from the top of the organisation through to field operations. This will require some cultural and mind-set adjustments and appointed cyber security responsibilities.
- A Technology Change Management strategy should be employed to address migrating legacy technology to smart grid technologies. This provides a controlled lifecycle of technology change management through evaluation, pilot, deployment and technology retirement lifecycle phases.
- A Technology Change Control Board should be introduced. This is an appointed management group which consists of stakeholders within the organisation that have dependencies in cyber security matters.

The main body and detail of the findings in this section are described in APPENDIX I - Organisation Level Smart grid Cyber Security Framework.

3 NEXT STEPS

This section presents a brief summary of recommended next steps towards addressing smart grid cyber security in the UK.

3.1 National Level

- Incorporate smart grid cyber security considerations into the work of the Smart Grids Forum, to be developed as a result of explicit recognition of the link between smart grid cyber security and security of supply;
- Identify organisational boundaries and interfaces between National Grid and Distribution Network Organisations with regard to cyber security roles responsibilities, and effective collaboration;

- Undertake smart grid cyber security risk assessment:
    - Agree on the use of IS1 to develop a national level risk assessment for smart grids;
    - Obtain the necessary clearance to use SMIP IS1 as input;
    - Develop and maintain a national level risk assessment for smart grids;
- Include smart grid cyber security as part of evaluation criteria for LCNF projects;
- Use the results of the risk assessment to inform/develop national level activities and to help inform/drive DNO activities;
- Review and update CPNI guides and tools with particular focus on requirements for smart grid cyber security.

3.2 Organisation Level

- DNOs to consider their risk assessment approaches and determine if appropriate for smart grid cyber security, and to consider the use of IS1 as an alternative;
- DNOs to explicitly consider cyber security on current and future LCNF projects;
- DNOs to consider their overall approach to technology change management, with a view to more formal adoption of an Operational Security Management System in line with the framework recommended in this report.
- Detailed audit of candidate DNOs to establish gaps in current practices and develop applicable operational security management system requirements, policies and controls to address cyber security.
- Develop and deploy an operational cyber security training programme.

3.3 NISTIR 7628 Summary

For convenience, APPENDIX J - NISTIR 7628 Summary, provides an outline of the contents of NISTIR 7628.

4 APPENDIX A - BACKGROUND

The present electricity supply system consists primarily of large, centralised and predictable sources of generation, and networks to enable power flow to uncontrolled (but reasonably predictable) demand. The present electricity networks are therefore designed to facilitate primarily unidirectional flow from generation to demand, and to cope with the relatively low levels of short term unpredictability in demand. The vast majority of UK generation uses fuels such as coal, gas and oil.

However, the Government and Ofgem is now driving the transition to a secure, safe, low carbon, affordable energy system in the UK (the "low carbon transition"). Binding targets for the reduction of greenhouse gas emissions are in place, and the decarbonisation of electricity supply will be a major contributor to the achievement of these targets. The decarbonisation of electricity supply requires the electricity network companies to address significant new challenges, such as:

- Facilitation of low carbon developments in generation, including intermittent generation connected at all transmission and distribution voltage levels;
- Facilitation of developments in supply, including new commercial arrangements for demand response and more localised balancing of supply and demand through localised energy storage;
- Facilitation of low carbon developments affecting consumption such as Electric Vehicle (EV) charging, and the introduction of microgeneration technologies such as photovoltaic (PV) panels to reduce consumption of network supplied energy;
- Ensuring continued security of supply whilst facilitating all of the above.

Therefore, the future electricity system needs to integrate many more forms of supply and demand, be managed in a much more dynamic manner, and continue to be robust. A core element of this system will be an electricity network which has the capacity to transfer significantly more energy between a diverse range of dynamically changing generators and consumers, whilst maintaining the balance between supply and demand at multiple levels within the network. In order to achieve this, significant developments are required in integrated and intelligent monitoring and control of the network, resulting in a dramatic increase in the distributed nature and the complexity of network monitoring and control systems. The resulting energy system is commonly known as the smart grid.

4.1 Smart Grid Monitoring and Control

One of the core requirements for smart grid operations will be monitoring and control of the transfer of energy in real time throughout the energy system, continuously balancing generation and demand. This differs from the present system in that generation and demand fluctuations will be the result of much more dynamic combination of prevailing physical, environmental, operational, commercial and market conditions. This requirement will be met by increasingly complex and sophisticated network monitoring and control systems in the form of:

- A small number of large high-level network control and monitoring systems for overall management of the smart grid, divided according to voltage levels as is currently the case (i.e., separate systems for each transmission and distribution network). However, increased coordination between these systems may be required, leading to requirements for greater intelligence and more advanced communications interfaces in order to achieve a higher degree of integration between the systems;
- A large number of small low-level network control and monitoring systems for localised management of portions of the smart grid. These will be required at the lower voltage levels and will require to be intelligent systems, with advanced communications interfaces in order to achieve the levels of integration required to share their data and coordinate their actions on a local level, and also to communicate with the high-level network control and monitoring systems;
- A large number of individual network connected smart grid devices, for localised measurement and control at specific points in the smart grid, also requiring embedded intelligence and advanced communications interfaces. This will include smart meters and smart appliances installed in domestic households, as well as industrial and commercial premises.

4.1.1 Smart Metering as an Element of the Smart Grid

Smart metering involves the installation of intelligent meters in consumer"s premises and a communications infrastructure to allow the meters to communicate with energy providers. This facilitates the collection of consumption related data at regular intervals, and the forwarding of that data to energy providers for billing and other purposes. The functionality of smart meters may also include remote disconnect capability or other controls, all via the smart metering communications infrastructure, and may also facilitate the integration of other smart appliances with the electricity supply system.

Smart metering therefore presents a major opportunity with respect to smart grid operation through the provision of time-based consumption information at end points on the electricity network, and the provision of an infrastructure which could support some network management operations. Therefore, smart metering can be considered a key component of smart grids, facilitating the participation of the domestic consumer in the overall smart grid as illustrated in Figure 1 below.

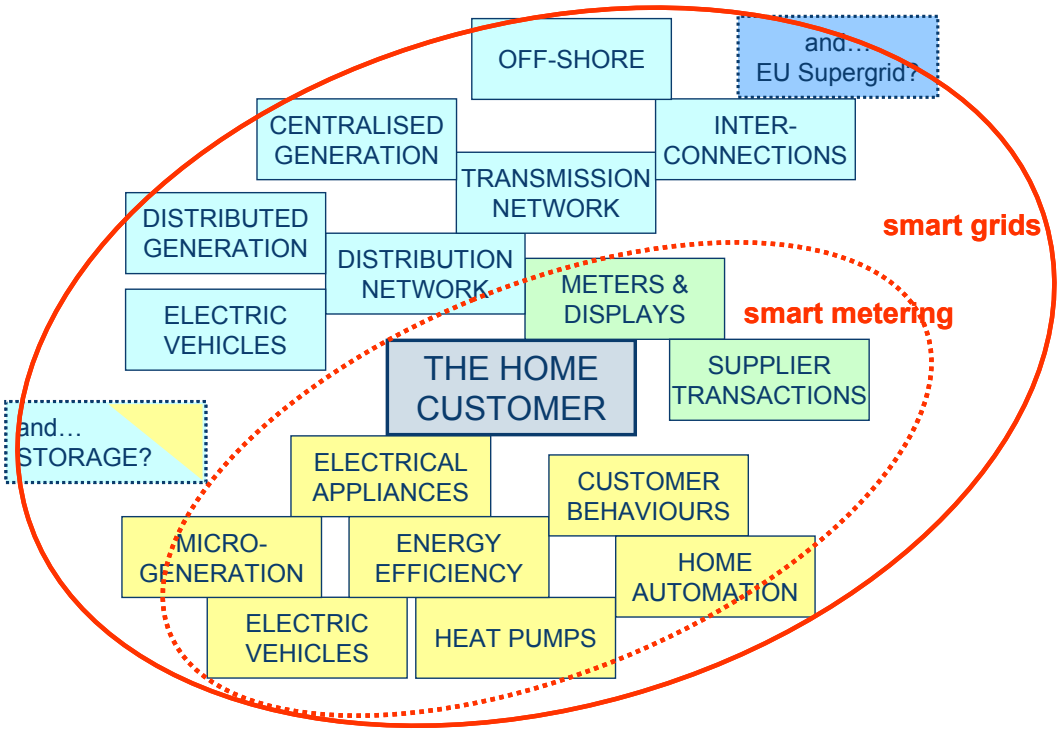

Figure 1 - Smart Metering as part of the Smart Grid Architecture

4.2 Critical National Infrastructure

The electricity network infrastructure, whether smart grid or traditional grid, is a fundamental requirement for the functioning of modern society. Its importance to daily life means that it is considered as one of the elements of Critical National Infrastructure (CNI), and it must be carefully designed, implemented and operated in order to ensure that risks to the proper functioning of this element of CNI are appropriately managed.

For the present electricity networks, Ofgem has set down standards that must be met by the network companies with respect to the performance of their networks, under all conditions.

The network companies assess and manage all risks to their operations to the extent required in order to satisfy these standards. The sources of these risks include both malicious activity (such as theft and vandalism) and non-malicious activity (such as accidental damage or equipment failure). The network companies also ensure that they have the appropriate means (resources, equipment, procedures, etc.) to recover as quickly as possible from situations when standards are not being met, for example due to power outages. These approaches need to be re-considered in the light of the evolution of this element of the CNI from present electricity networks towards the smart grid.

4.2.1 **Smart Grid Cyber Security**

The network monitoring and control systems required for smart grids described in section 4.1 will be delivered using computing systems built using advanced information and communications technology (ICT), which will allow smart grid control to be automated to a significant degree. Thus, the successful operation of the smart grid will be highly dependant on ICT-based computing systems, which will need to be sufficiently dependable such that they do not negatively impact on security of supply.

Dependability of a computing system is defined[1] as the ability to deliver service that can justifiably be trusted. The definition of dependability encompasses security and is the property of the computing system that integrates such attributes as:

- Availability - readiness for correct service;
- Reliability - continuity of correct service;
- Safety - absence of catastrophic consequences on the user(s) and the environment;
- Confidentiality - absence of unauthorized disclosure of information;
- Integrity - absence of improper alterations of system state;
- Maintainability - ability to undergo modifications and repairs.

More specifically, computing system security is the concurrent existence of:

- Confidentiality as defined above;
- Integrity, with „improper" as used in the above definition meaning „unauthorized"; and
- Availability, as defined above, with the additional requirement that this should be for authorized users only.

[1] A. Avizienis, J.-C. Laprie and B. Randell: Fundamental Concepts of Dependability. Research Report No 1145, LAAS-CNRS, April 2001

Thus, computing system security, along with computing system reliability, safety and maintainability, are critical attributes for smart grid implementation and operation, and need to be considered as part of overall risk management for this CNI.

Smart grid ICT will also enable a dramatic increase in the granularity of data available for smart grid monitoring and control purposes, both in terms of measurement points and measurement frequency, resulting in massive increases in data volumes. As this data will now include individual customer data, the issues of data security and data privacy become relevant for smart grid implementation and operation. Therefore, additional threats of information leakage and fraud must be considered for this CNI.

Collectively, smart grid computing system security and smart grid data security and data privacy are often referred to as smart grid cyber security.

Cyber security risks in general, and smart grid cyber security risks in particular, are not particularly well understood or quantified. This is the case for a number of reasons, principally:

- There is not a significant evidence base upon which to undertake quantitative analysis. Cyber security incidents involving impact on physical processes such as electricity network management have not been particularly numerous, and due to sensitivities regarding disclosure of such incidents it is likely that only a proportion of the total number of incidents are in the public domain;
- Cyber security risks arise due to threats which change over time. The sources of threats, and the people who carry them out (whether motivated to do so or by accident) constantly changes for any computer system as its configuration changes, its user base and their motivations change, and it is exposed to an ever changing external environment to which it is connected (such as the Internet). The fact that the smart grid forms part of the CNI will also increase interest levels from threat sources who would seek to cause impact to systems of such significance. These result in what is known as the dynamic threat model for smart grid cyber security;
- Computing systems are often highly complex systems, which engage in highly complex interactions with users and with other computer systems. In some cases computing systems have not been designed to be secure, for example in older systems where cyber security was not recognised as an issue. In other cases, computing systems are designed to be secure, but over time new cyber security vulnerabilities are discovered. Each new vulnerability has to be discovered, disclosed, fixed, assessed for applicability in each application, and then the fix

applied to every relevant instance of that application, in order for it not to increase cyber security risk.

The consequence of the above is that smart grid cyber security risks can only be qualitatively assessed, need to be re-assessed on a regular basis as the threat landscape changes and new vulnerabilities are disclosed over time, and need to be actively managed to maintain acceptably low levels of risk. Part of the purpose of this report is to inform the Energy Networks Association (ENA) and the Department of Energy and Climate Change (DECC) on what should be done to address these challenges.

4.3 Current Status of UK Smart Grid Implementation

The UK has already started the process that will make smart grids a reality. Key initiatives include:

- The Electricity Networks Strategy Group (ENSG), which provided a forum bringing together key smart grid stakeholders, and was chaired jointly by DECC and Ofgem. The ENSG published a vision and a smart grid routemap between 2009 and 2010. Most recently, DECC and Ofgem have commenced the establishment of the Smart Grids Forum, which will focus on the issues of network development as a key part of the low carbon transition;
- The Smart Metering Implementation Programme (SMIP), which will result in the rollout of smart electricity and gas meters to all homes in GB by 2020;
- The Low Carbon Network Fund (LCNF), through which Ofgem is providing £500m over the five year period 2010 - 2015 to support smart grid trials being delivered by the DNOs, along with DECC's funding of smaller smart grid demonstration projects through the Low Carbon Innovation Fund.

5 APPENDIX B - APPROACH

Over recent months the ENA has had discussions with DECC on the topic of cyber security for smart grids, and DECC has suggested that work done to date by organisations internationally such as the National Institute of Standards and Technology (NIST) in the US, and the EU Task Force on Smart Grids, could be used as a basis to develop a high-level approach to managing the cyber security issue in the context of smart grid deployment in the UK. Such an approach could incorporate a management framework for smart grid cyber security, including a risk assessment strategy applicable to the UK.

Further to those initial discussions, DECC asked the ENA to undertake the work required to review international initiatives and outline a framework which adapts those international initiatives to suit the UK environment for smart grids. The ENA Electricity Networks and Futures Group (ENFG) agreed to undertake the work, and invited KEMA to deliver the work on its behalf.

5.1 Approach Development

The smart grid requires end-to-end measurement, control and communications to an extent which simply does not exist in current electricity networks, and which will require a holistic approach to managing cyber security. However, KEMA's experience is that cyber security management approaches for the current electricity network architecture have a tendency to be somewhat fragmented, with responsibility for cyber security and any associated management systems split across different parts of the electricity networks companies' businesses. The complexity of this situation is also increasing with the introduction of smart metering, as both energy suppliers and the Data Communications Company (DCC) will become parties with responsibilities for elements of the smart grid architecture. From a networks perspective, cyber security responsibilities based on present electricity networks and the introduction of smart metering can be illustrated as shown in Figure 2 below.

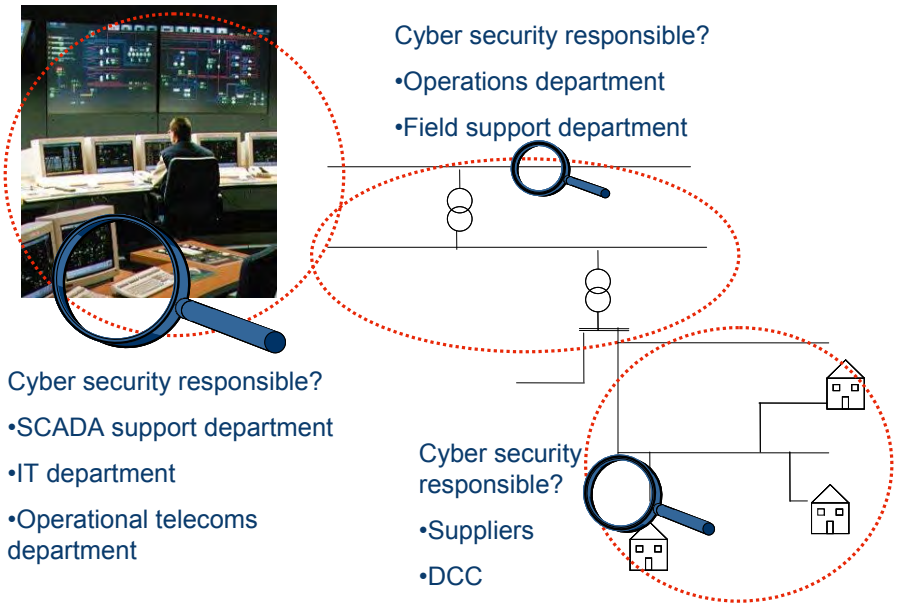

Figure 2 - Current Network Architecture and Cyber Security Responsibilities

In comparison, Figure 3 below illustrates the requirement for a holistic smart grid cyber security approach, with an overall management system and responsibilities which cover all aspects of the smart grid.

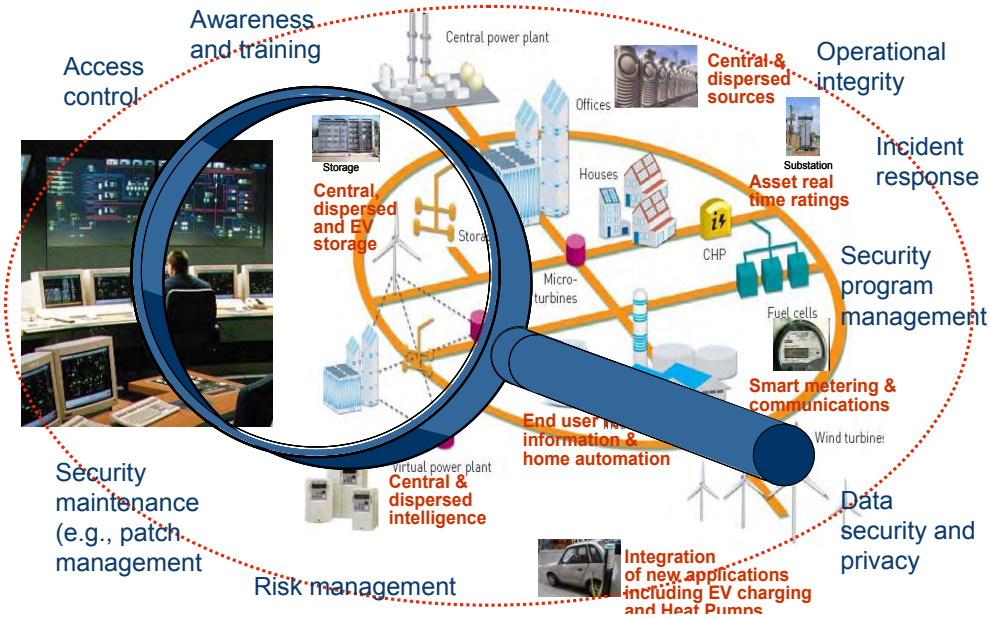

Figure 3 - Smart Grid Architecture and Cyber Security Responsibilities

The above suggests that there will be significant work to do to ensure that smart grid cyber security encompasses the full end-to-end architecture.

The approach to this project recognises the current situation as described above, and that there are activities and initiatives already under way in the UK which are relevant to smart grid cyber security, namely smart metering cyber security and electricity network operational systems cyber security:

- Smart metering cyber security typically focuses primarily on addressing data security and privacy in order to ensure that consumer privacy is upheld and data protection requirements are met. It also ensures that the control functionality included in some smart metering specifications (e.g., remote disconnect) is secure.
- Electricity network operational systems cyber security focuses on securing the operational technology (i.e., systems used for real-time control and management of electricity networks, also known as SCADA/EMS/DMS systems). These systems typically provide centralised control of the geographically distributed network infrastructure, with limited distributed intelligence.

This is illustrated in Figure 4 below.

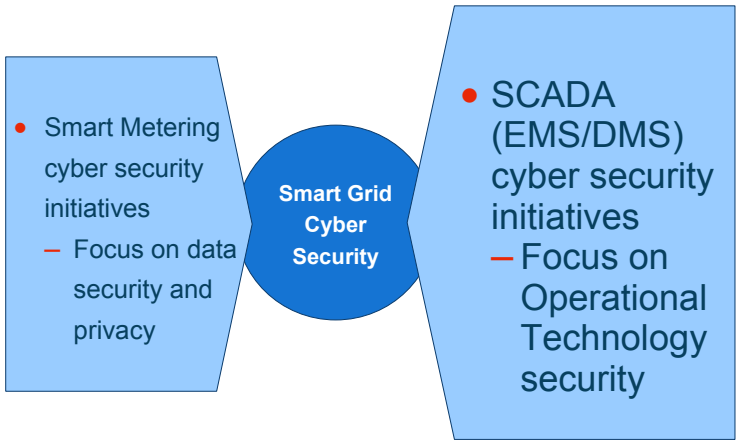

Figure 4 - Smart Grid Cyber Security Inputs

It is considered that electricity network operational systems cyber security has a closer alignment with smart grid cyber security than smart metering cyber security, primarily because the smart grid is an evolution of the present electricity network architecture, as described in section 4.1. However, it is recognised that the smart metering infrastructure will be a key extension to that architecture in terms of both measurement and control, as described in section 4.1.1. It is therefore logical that electricity network operational systems

cyber security should play a significant role in the development of smart grid cyber security approaches, as depicted in Figure 4 above, and that smart metering cyber security should also be an important factor.

In order to make best use of existing industry practice and the outputs of related initiatives already underway internationally and in the UK, the project includes a review of international smart grid cyber security initiatives and their outputs (e.g., NISTIR 7628, EU Task Force on Smart Grids), as well as a review of the network companies' current initiatives related to cyber security for their existing electricity network operational systems. Furthermore, relevant cyber security elements of the Smart Metering Implementation Programme (SMIP) in GB are also incorporated, recognising the interdependencies between smart metering and smart grids as a whole.

5.2 Scope of Work

The scope of work is based on the approach outlined above and includes activities which seek to ensure that any framework to address smart grid cyber security for the UK is consistent with these other relevant current initiatives and existing standards and guidelines. The scope of work is therefore as follows:

- Engage with key stakeholders in the UK to establish an overview of current activities that could be relevant to smart grid cyber security. Stakeholders include:
    - DECC (including the Energy Emergencies Executive Committee (E3C)); No response to date regarding any specific concerns of E3C with respect to smart grid cyber security, however, this should be pursued.
    - Cabinet Office – Office of Cyber Security; CPNI are exploring the possibility of setting up a meeting. This should be pursued.
    - The Centre for the Protection of National Infrastructure (CPNI), including the SCADA and Control Systems Information Exchange (SCSIE);
    - Electricity network companies;
    - The GB Smart Metering Implementation Programme (SMIP);
- Identify, through the discussions with UK stakeholders above, current activities as a result of European directives and other initiatives such as:
    - EU directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (2008/114/EC);
    - EU Task Force on Smart Grids, specifically Expert Group 2 (EG2) outputs related to data safety, data handling and data protection;

    - Review NIST Guidelines for Smart Grid Cyber Security (NISTIR 7628) and develop an understanding of how the cyber security issue could be handled in the context of smart grids deployment in the UK based on the NIST guidelines;
- Identify other UK standards and guidelines which could also provide valuable input to the development of a framework to address smart grid cyber security in the UK. In particular, aspects of the following standards/guidelines were considered:
    - CPNI's Good Practice Guides for Process Control and SCADA Security;
    - NICC ND 1643 Minimum Security Standards for Interconnecting Communications Providers;
- From the inputs above, develop a high-level approach to address smart grid cyber security for the UK, including a framework for risk assessment.

5.3 Scope of Document

This document is the final report from this project, and is intended to provide a sound basis upon which detailed and enduring smart grid cyber security efforts can be built. Proposals are provided at two levels: firstly at national level to provide an overarching approach to smart grid cyber security, and secondly at DNO level to support the development of management systems for smart grid cyber security.

6 APPENDIX C - CURRENT UK ACTIVITIES

6.1 Government

DECC has actively addressed the cyber security issue as part of the Smart Metering Implementation Programme, and this is discussed in more detailed in section 6.4 below. Aside from that, DECC has recognised the need to incorporate cyber security considerations into UK smart grid developments from the earliest possible stage. This has been demonstrated through the ENSG, particularly in their routemap[2], where the need for a prioritised, coordinated and concerted approach to security is emphasised. Within the routemap document, the potential challenge due to security threats and data protection risks is identified, along with the need to address this via the management of perceptions and the building of security and resilience into the core of the solution.

In the more detailed sections of the routemap document, four smart grid project types are identified: individual technology; multiple integrated technologies; customer and technology integration; and end-to-end integration. Cyber security is identified as a potential sub-project within multiple integrated technologies projects and customer and technology integration projects specifically, rather than as challenge to be addressed within all four project types. This perception of the cyber security challenge is perhaps somewhat narrower than it needs to be in order to ensure that cyber security is actively addressed for all aspects of smart grid developments.

The ENSG also suggests that centralised security management and ongoing threat/vulnerability evaluation and response are potential elements of the routemap as part of the activities to trial integrated technology at scale. However, it is not clear the extent to which centralised security management could be delivered, based on the assumption that the smart grid will be delivered by a range of interoperable architectures, owned and operated by multiple parties, rather than a single architecture.

[2] Electricity Networks Strategy Group – A Smart Grid Routemap, February 2010

Most recently, DECC and Ofgem have decided to establish the Smart Grids Forum, which will focus on the issues of network development as a key part of the low carbon transition. The Forum will need to consider strategic issues and key future network challenges (with a particular focus beyond 2020), including questions of network innovation, system balancing strategies and the roll out of smart grid technologies. Further details of the range of topics to be covered the Smart Grids Forum are yet to be announced.

6.2 Regulatory Policy

Ofgem promoted the importance of smart grids in the last electricity distribution price control review (DPCR5) that took effect in April 2010 with the announcement of the Low Carbon Networks Fund (LCNF). In the period from April 2010 to the end of March 2015, the LCNF allows up to £500m of support to projects sponsored by the DNOs to try out new technology, operating and commercial arrangements. The objective of the projects is to help all DNOs develop their understanding of what they need to do to provide security of supply at value for money as GB moves to a low carbon economy.

The LCNF Governance Document[3] sets out details of the regulation, governance and administration of the LCNF, including eligibility/evaluation criteria for projects. The criteria are focused in trialling new commercial or operational arrangements, or new technologies, on the distribution system, which accelerate the development of low carbon energy, have the potential to deliver net benefits to customers, and generate new knowledge that can be shared amongst DNOs. Requirements related to smart grid cyber security are implicit, in that the overarching objective of LCNF projects is to trial solutions which can provide security of supply in a low carbon economy, and smart grid cyber security in the context used in this report is implicitly a contributing factor to security of supply.

Network innovation is expected to play an even larger part in the next electricity distribution price control review, which will commence in 2012 and be implemented in 2015. For this price control, Ofgem will replace traditional RPI-X based regulation with a new regulatory framework RIIO, where RIIO stands for Revenue=Incentives+Innovation+Outputs. RIIO will be based on an eight-year price control period, compared to the current five-year period. RIIO will also expand on the LCNF by introducing a new innovation stimulus to further encourage the growth of smart grids.

[3] Ofgem, LCN Fund Governance Document v.3, 22 July 2010

6.3 CPNI

CPNI is the government authority that provides protective security advice to the national infrastructure, and recognises that SCADA security is one of the key issues for national infrastructure protection. It supports industry in addressing SCADA security in a number of ways:

- Providing security advisories and vulnerability disclosure information to industry. This includes the provision of information and other awareness raising activities targeted at senior industry executives;
- Developing and issuing a suite of good practice guidance documents, providing recommendations for process control and SCADA security. These good practice guides were originally issued by CPNI's predecessor, the National Infrastructure Security Co-ordination Centre (NISCC), and are now well-established and mature. Additionally, CPNI publishes guidance regarding personnel security;
- Establishing the SCADA and Control Systems Information Exchange (SCSIE), a confidential industry-CPNI forum that meets regularly to exchange information on SCADA threats, incidents and mitigation. Membership of the SCSIE includes representatives from companies that own and operate UK critical infrastructure using SCADA and process control systems, including energy, transport and water companies.

Whilst CPNI does support the electricity network companies in benchmarking their own cyber security practices against the published good practice guides, and covers a range of relevant SCADA security topics in SCSIE meetings, there are no specific smart grid cyber security initiatives in this area.

CPNI is also active in supporting and driving awareness raising activities within industry, and in the context of the SCSIE this includes support to help ensure that cyber security for process control and SCADA systems is a topic which is raised to executive level.

6.3.1 Good Practice Guides - Process Control and SCADA Security

There is no single international standard for which compliance will deliver appropriate SCADA security. Instead, there are a number of relevant standards and guides available, one series of which is the CPNI good practice guides on Process Control and SCADA Security. Similarly with other guidelines/standards, the CPNI guides recommend the following SCADA security activities:

- Implement an overall SCADA security management/governance system, including policies, organisational structure with clearly defined roles and responsibilities, management reviews, exception handling and compliance monitoring;
- Understand the business risks and put in place an ongoing programme of risk management;
- Understand the nature and details of dependencies on third parties, and manage third party risks;
- Implement secure architecture, both on new projects and existing systems, and put in place an ongoing programme of monitoring and reviewing security. Implementation includes technical, procedural and management measures;
- Implement appropriate procedures for personnel, including training to improve awareness and skills;
- Implement an appropriate incident reporting plan and response planning.

6.3.2 Process Control and SCADA Security Benchmarking

Benchmarking activities are undertaken by CPNI on an annual basis, via an Excel spreadsheet based SCADA Self-Assessment Tool (SSAT), which each company is invited to complete and return. The purpose is to provide CPNI and participating organisations with a high level information assurance assessment of SCADA/control systems. KEMA has had sight of the SSAT spreadsheet[4] but has not had sight of any completed self-assessment questionnaires or of benchmarking results, so the comments below are based purely on the SSAT itself.

The SSAT maps clearly onto the CPNI Good Practice Guides, and is therefore designed to provide a view of the degree to which the companies follow the practices defined in the Good Practice Guides. The coverage of the SSAT includes two broad categories of systems within the control systems environment: Industrial Control Systems (ICS), which includes SCADA, and telemetry. Companies are invited to complete separate questionnaires for each category of system.

[4] CPNI SCADA Self Assessment Tool Version 3.0 May 2010

6.4 Smart Metering Implementation Programme

The Smart Metering Implementation Programme (the Programme) is the central programme for the rollout of electricity and gas smart meters across Great Britain (GB), currently being delivered by Ofgem e-serve on behalf of DECC. The Government and Ofgem published a smart metering prospectus in July 2010, for consultation. The prospectus set out proposals for how smart metering will be delivered, including design requirements, central communications, data management and the approach to rollout. The consultation is now closed, and the response to the consultation is expected to be published in March 2011. In parallel with the consultation process, Programme workstreams have been progressing with the development of detailed specifications, which will be completed in June 2011.

Within the Programme, security is of prime concern. Basic security requirements were established in the prospectus, and these are being further developed by the Programme Team with input from the Programme's Privacy and Security Advisory Group (PSAG), who provide advice in the context of data privacy and security. In addition to this, the current phase of the Programme (phase 1a) has recognised the need to obtain input on wider cyber security concerns related to smart metering, covering technical and operational security and security governance issues, and supporting the requirement to follow "security by design" principles. This has led to the establishment of the Smart Metering Security Technical Experts Group (STEG), to support the Programme by:

- Providing advice on the governance of security risks, and the risk mitigation strategies for the design, implementation and operation of systems proposed by the Programme Team;
- Actively identifying and supporting the assessment of security risks and threats across the Smart Metering Design, Data Communications Company Design and Rollout workstreams;
- Providing a forum where those security matters can be discussed and advice can be provided on mitigating security risks and threats identified;
- Helping the Programme Team to understand the impact of security issues on the Smart Metering Implementation Programme and all stakeholders; and
- Using the group to share information emerging from European forums discussing security to ensure the Smart Metering Implementation Programme is aware of European initiatives.

The STEG operates in an advisory capacity and has no decision-making powers.

The Programme recognises that security risk assessment and wider risk management activities must be embedded into the Programme throughout its lifecycle. Recognising that there are many security risk assessment and risk management methodologies available, the Programme has decided to utilise the methodology which is mandated by the Security Policy Framework (SPF)[5], a Cabinet Office published approach which provides central internal protective security policy and risk management for Government Departments and associated bodies. Whilst the SPF is aimed primarily at Government Departments and Agencies in supporting its protective security and counter-terrorism responsibilities, it does have wider application, particularly with the parts of the commercial sector which make up the core sectors within the CNI. For this reason, and although not mandated to do so, the Programme elected to meet SPF Mandatory Requirement 32, which states: "Departments and Agencies must conduct an annual technical risk assessment (using HMG IA Standard No.1[6]) for all HMG ICT Projects and Programmes and when there is a significant change in a risk component (Threat, Vulnerability, Impact etc.) to existing HMG ICT Systems in operation. The assessment and the risk management decisions made must be recorded in the Risk Management and Accreditation Documentation Set (RMADS), using HMG IA Standard No.2 - Risk Management and Accreditation of Information Systems."

At the time of writing, the Programme has completed an initial risk assessment and has received comments from the STEG. A further iteration of the risk assessment will be undertaken in March 2011, and the Programme is planning to proceed with risk management and accreditation work using HMG IA Standard No. 2.

Phase 1a of the programme is due to complete in March 2011, at which point the programme will be handed over from Ofgem e-serve to DECC to deliver phase 2 onwards. The ongoing structure and governance of the programme has been agreed in principle between Ofgem e-serve and DECC, and this includes the scope of the STEG's involvement in the ongoing programme to ensure that security issues are being raised and addressed appropriately at the various working groups that will continue developing the detailed specifications for release in June 2011.

---

[5] Her Majesty's Government Security Policy Framework, v.4.0, May 2010

[6] Her Majesty's Government Information Assurance Standard No. 1 - Technical Risk Assessment, October 2009, Issue No: 3.51

6.4.1 **HMG IA Standard No.1 – Technical Risk Assessment**

HMG IA Standard No.1, commonly known as IS1, provides a method to identify and assess the technical risks that an ICT system is exposed to. The key output is a list of prioritised risks that can be used as a basis for risk treatment requirements and options for managing the risks. The standard aligns well with international standards, notably the ISO 27000 series.

IS1 states that risk assessment is an ongoing process that must be carried out within the broader context of the risk management and accreditation process, as described in HMG IA Standard No.2 (commonly known as IS2).

The key concepts used in IS1 are as follows:

- The scope of the risk assessment covers three different aspects of the ICT system being assessed (or of the project to deliver the ICT system). These are:
    - Accreditation Scope, which includes all of the capability and services for which the system or project is responsible for delivering;
    - Reliance Scope, which identifies capability and service not supplied by the system or project directly, but which the system or project relies upon. This would include third party supplied products and services;
    - Analysis Scope, which includes both the Accreditation Scope and the Reliance Scope, plus any business information exchange requirements and system connections;
- The methodology is asset focused, so the system being assessed must be split into assets. Assets are defined as „anything, which has value to an organisation, its business operations and its continuity". Assets can be grouped into collections known as Foci of Interest (FoI) to simplify the assessment process. The methodology also includes an optional modelling technique to assist in understanding the system being assessed;
- The methodology defines that the impact of compromises of confidentiality, integrity and availability of an asset are to be analysed and a Business Impact Level (BIL) assigned on a seven point numerical scale from 0 to 6. Assignment of BIL is a business led decision;
- The standard distinguishes threat sources from threat actors:
    - A threat source is a person or organisation that desires to breach security and ultimately will benefit from the breach in some way;
    - A threat actor is a person who actually performs the attack or, in the case of accidents, will cause the accident;

Authorised users can be threat sources and threat actors. All threat actors belong to one or more threat actors types, which are defined in the standard;

- Analysing the combination of capability and motivation of a threat actor or threat source to attack an asset results in the assignment of a threat level;
- Compromise methods are defined in the standard, based on threat actor types, and define the broad type of attack by which a threat actor may attempt to compromise the confidentiality, integrity or availability of an asset;
- Risk is defined as the likelihood that a threat will exploit a vulnerability leading to a business impact. IS1 is designed to support the identification of all technical risks and estimate a risk level for each one. Within IS1, each risk consists of a number of components:
    - Threat actor and threat actor type;
    - Threat source;
    - Compromise method;
    - Identification of which property/ies (confidentiality, integrity or availability) of an asset or FoI are compromised, and the BIL associated with the compromise;
- Risk level is a combination of threat level and BIL. The elements of likelihood and vulnerability cannot be assessed in a generic sense and in the early stages of a risk assessment may not be known. Risk level is defined on a six point scale.

The standard defines a six-step process for risk assessment, as illustrated in Figure 5 below.

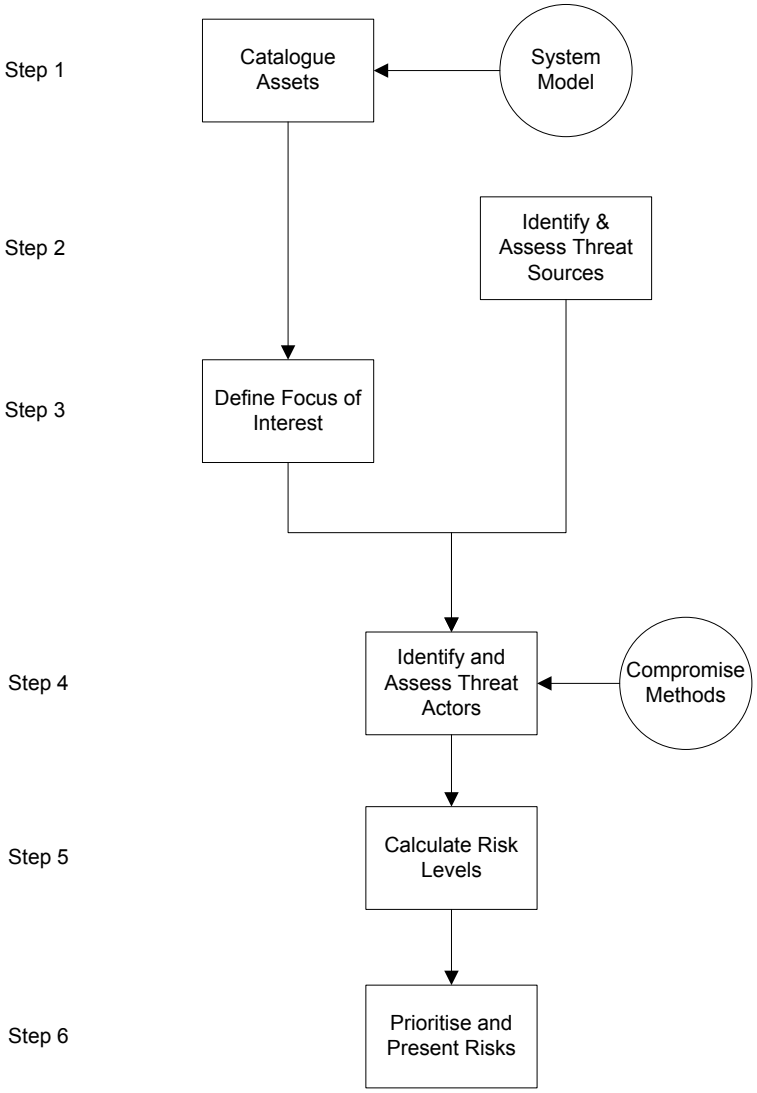

Figure 5 - Risk Assessment Method

6.4.2 Smart Metering Implementation Programme Risk Assessment

Specific information related to the risk assessment for the Smart Metering Implementation Programme is classified as restricted, and therefore cannot be shared in this report. However, it should be noted that the scope of the risk assessment was defined using Steps 1 and 3 of IS1, so is based on a catalogue of assets within scope, and consequent Foci of Interest. The assets within scope were therefore based on the scope of the smart metering system and the entities on which it will be dependant, as illustrated in Ofgem's Statement of

Design Requirements[7]. This is replicated in Figure 6 below with some additional detail regarding dependencies on other industry parties.

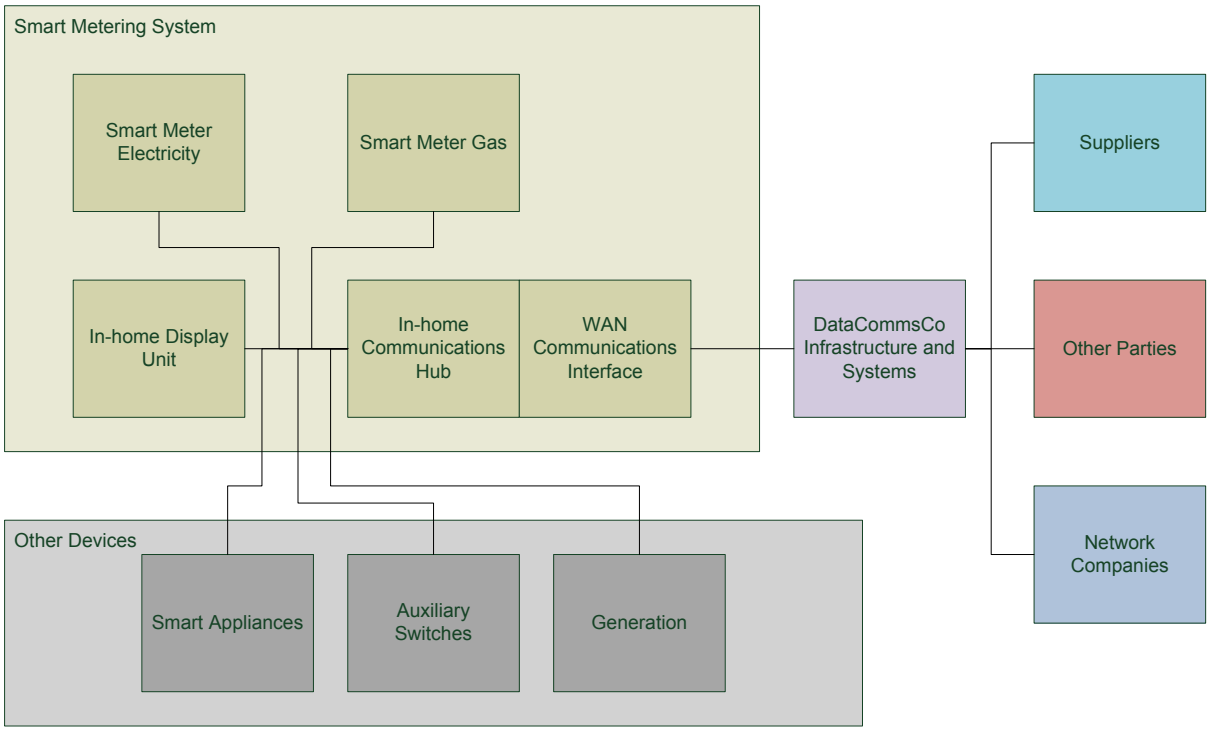

Figure 6 - Asset based Risk Assessment Scope for Smart Metering

Note that the other devices shown in the diagram above are only in scope with respect to the communications interfaces, and not with respect to functionality and performance of the devices.

6.4.3 DCC Governance

As can be seen from Figure 6 above the DCC will be the single entity responsible for delivering central data and communications activities for smart metering, integrating and managing all meter data with respect to provision of the appropriate data (and services) to suppliers, network companies and other authorised parties. The DCC will be subject to a governance framework which will include a licence, and a new Smart Energy Code to which

[7] Figure 1 – Scope of Functional Requirements Catalogue, from Statement of Design Requirements, Ofgem, Document Ref: 94b/10, 27 July 2010.

it will obliged to be a party. The licence and Code will not specify the technology or technologies to be used for WAN communications but rather will set out the functional, including security, requirements of the end-to-end communications system.

6.5 Key Observations

Further details of the range of topics to be covered by the DECC/Ofgem co-chaired Smart Grids Forum are yet to be announced, however it is clear that smart grid cyber security will need to be a significant consideration for the Forum.

In ENSG and LCNF published material, whilst smart grid security may be recognised as a challenge, the nature of the relationship between overall security of supply and smart grid cyber security appears to be implicit rather than explicitly stated. This could lead to misunderstanding of the existence of such a dependency, and a consequent lack of focus on smart grid cyber security as an issue which must be addressed in order to help ensure security of supply. The introduction of the concept of dependability of the smart grid, as detailed in section 4.2.1, and the clear definition of the relationship between smart grid dependability and security of supply, would perhaps permit a more explicit dependency to be defined and therefore the importance of smart grid cyber security to be understood in its widest context.

CPNI's Good Practice Guides appear to be well utilised at operational management levels and below in industry. However, whilst this is the case and whilst CPNI supports awareness raising up to executive level, there are indications that the level of executive support is not as high as it should be. With respect to smart grid cyber security, demonstration of clear dependency between smart grid cyber security and security of supply should help develop the appropriate levels of executive support.

CPNI's self-assessment approach to process control and SCADA security clearly provides some useful information which can be shared amongst the industry. However, the fact that companies are invited to complete separate questionnaires for each category of system, such as SCADA and telemetry, could mask some issues with regards to a holistic approach to operational systems cyber security across the organisation. If this same self assessment approach were to be used for smart grid cyber security, weaknesses due to different approaches between for example those responsible for communications and those responsible for field devices may not be apparent. Therefore, the use of such tools for smart

grid cyber security assessment should be repositioned to assess smart grid cyber security on a more holistic basis.

The use of IS1 as the method of risk assessment for the SMIP has been widely welcomed, and a similar approach for smart grid risk assessment should be considered.

Cyber security requirements for the smart metering system will be defined in the detailed specifications for the smart metering system, and cyber security requirements for the communications infrastructure being delivered by the DCC will be defined in the DCC licence and the Smart Energy Code. These provide ideal places for cyber security requirements to be stated, and benefit from the fact that there will be one set of detailed specifications which will be applicable to all suppliers participating in the rollout, and one wide area communications infrastructure provider. This situation will not exist for the smart grid deployment, with each DNO responsible for deploying its own smart grid solutions, including communications infrastructure, to its own specifications. Therefore there is a greater challenge to the coordination of smart grid cyber security efforts.

7 APPENDIX D - ELECTRICITY NETWORK COMPANY ACTIVITIES

KEMA met with a number of electricity network companies (all DNOs) in order to build an overview of current activities that could be relevant to smart grid cyber security. Particular areas of focus for the discussions with these companies were:

- Approach to cyber security for existing operational network management systems and processes;
- Approach to cyber security on projects to implement changes to existing operational network management systems and processes;
- Approach to cyber security on innovation and pilot/demonstration projects for smart grid systems and processes.

The discussions were held with volunteer DNOs, and details of company specific approaches were shared. However, as the purpose of these discussions was to build a representative picture of relevant approaches and activities within the industry, this report does not attribute any specific finding or observation to any of the companies interviewed.

7.1 Current Operational Network Management Systems and Processes

The DNOs all recognise the critical nature of the infrastructure that they own and operate, and are very focused on maintaining the availability and quality of the services they provide, as would be expected. Therefore, their organisational structure, operational systems and business processes are all geared towards the delivery of safe and reliable electricity supplies.

Several factors contribute towards the achievement of these operational objectives, including planning, designing and building an appropriately robust electricity network infrastructure, comprising reliable assets which are appropriately utilised and cared for, operating the network on a round the clock basis to ensure continued supply under all operating conditions, and reacting appropriately when action needs to be taken to maintain or restore supplies. Currently, the key systems for real time electricity network monitoring and control are the central SCADA/DMS systems, the equipment in substations and at other points in the network that collect network data and allow the network to be remotely controlled from the SCADA/DMS systems, and the wide area communications infrastructure that facilitates the

exchange of data (both monitoring and control data) between them. In order to support operational network management, the SCADA/DMS systems also interface to other systems such as outage management, asset management, and geospatial information systems, which are often considered as "corporate applications" in that they do not directly control the network and are located on the corporate data network which is separated from the SCADA data network.

Ownership and management of the various real time electricity network monitoring and control systems is often split across various parts of the DNOs businesses, typically following the pattern below:

- Electricity network operations. Responsible for the actual operation of the electricity network, owner of the SCADA/DMS assets, and owner and manager of the remote equipment assets;
- IT. Responsible for the management of the SCADA/DMS, and owner and manager of the wide area communications infrastructure;
- Asset management. Owner of the remote equipment assets.

This typical arrangement is illustrated in Figure 7 below.

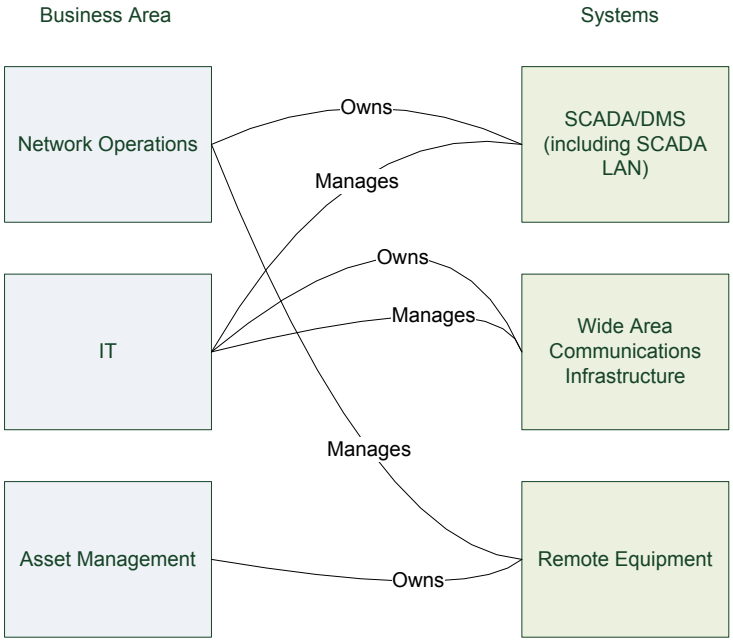

Figure 7 – Typical Ownership and Management of Operational Network Management Systems

7.1.1 Governance Arrangements

The arrangements shown in Figure 7 above mean that well-defined relationships need to be in place to ensure appropriate governance of the systems, and this is generally the case. For example, no changes are made to the SCADA/DMS by IT, unless the change is approved by Network Operations. Also, IT will typically ensure, via its own internal governance procedures, that proposed changes to the wide-area communications infrastructure must be approved by an appropriately authorised person (who cannot be the same person that raised the proposed change in the first instance).

However, there are some potential areas of risk apparent within these arrangements. Whilst governance arrangements are generally well established and robust for systems which are typically identified as IT systems (including communications), these are less evident for systems which are not typically identified as IT systems. Such systems include a significant proportion of what is defined in Figure 7 as remote equipment, including substation installed Remote Terminal Units (RTUs) and also other automation equipment and devices located both inside substations and also as stand-alone network equipment. In current operational network management systems, this type of equipment often has limited intelligence and configurability or re-programmability, with configuration changes performed locally on-site by connecting a laptop with specialist software installed which provides the capability to re-programme the equipment. However, the laptops, the programming software on the laptops, and the programmes which are being altered on the equipment itself, are often governed only by the field engineers undertaking the work. It should be noted that any activity undertaken by an engineer in this environment is fully governed by procedures to ensure that operational and safety risks are appropriately managed.

Another feature of this type of equipment installed today is that its communications capabilities are often very limited. Although it will need to communicate with the SCADA/DMS systems through the wide area communications infrastructure, it will often do so using proprietary point-to-point protocols over low bandwidth communication media such as radio, microwave, dial-up PSTN or leased line telecommunications. This naturally limits the scope for large scale impact upstream on the electricity network as a result of a problem with the remote equipment; typically the impact will only be downstream of the remote equipment, such as a localised outage. However, more modern remote equipment has the capability to use open standard routable protocols over higher bandwidth communication

media including mobile telecommunications technologies such as GPRS, which increases the risk as there is a greater potential for large scale upstream impact on the electricity network as a result of a problem with the remote equipment. Poor governance arrangements in this area mean that these increased risks may not be appropriately managed.

A key observation in this area is that if equipment is not considered to be IT or SCADA equipment, then it will not be governed in accordance with IT or SCADA best practices. In this context SCADA is often considered to be only the central SCADA/DMS system and the associated communications infrastructure.

7.1.2 **Risk Management**

The DNOs typically have very well established enterprise risk management approaches, enshrined in corporate policy. These are supported by risk management procedures which coordinate and consolidate risk assessment activities, providing a regularly updated corporate picture of risk across the enterprise. Within operations, risk assessment is focused on familiar risk areas such as physical, environmental and safety risks. Within IT, risk assessment is focused on other familiar risk areas such as security, availability and performance.

This situation gives rise to two observations:

- Cyber security risk assessment for operational network management systems is an intersection of the scope of operational risk assessment and IT risk assessment. In general, this appears to be recognised only at an informal level and not at the enterprise level (i.e., this intersection is not recognised at enterprise level as being a key area for risk management efforts);
- In line with the comments made previously concerning the generally poorer governance of remote equipment, such equipment may not be receiving enough consideration as part of cyber security risk assessment efforts for operational network management systems.

7.1.3 **Awareness and Training**

DNOs do take awareness and training on a range of topics very seriously for all personnel. Health and safety, physical security (e.g., bomb threats) and other relevant topics are all

covered in induction programmes as well as on-going awareness and training programmes. However, awareness and training concerning operational network management systems cyber security does not appear to be well covered across the DNOs. Generic elements such as IT security are well covered, but specific awareness raising or training concerning operational network management systems cyber security is not.

Awareness and training resources such as posters and videos are available from CPNI, but these are not widely utilized throughout the DNOs. For example, in one case the CPNI video had been shown to call centre and control centre personnel, but not to field-based personnel.

7.1.4 Security Requirements

Up until a few years ago it was not unusual that requirements specifications for new operational network management systems would contain no security requirements at all. This has now changed, with the DNOs much more keenly aware of the need to include security requirements in specifications for new systems. Publicly available resources such as the Cyber Security Procurement Language[8] are now being used by DNOs. However, in line with other observations, the use of these resources appears to be most prevalent for specifying major systems such as SCADA/DMS, and are less well utilized for field-based equipment.

7.2 Innovation and Pilot/Demonstration Projects for Smart Grid Systems and Processes

Outside of the operational environment, new technologies, systems and related processes are constantly being developed for electricity network management applications. This has accelerated over recent times as new smart grid related technologies and systems are developed and actively marketed. The DNOs increasingly recognise the need to innovate with respect to the development and adoption of these new smart grid related technologies and systems, and have developed their own innovation approaches. This has been bolstered in GB by the LCNF, through which innovation and pilot projects can be funded.

[8] Department of Homeland Security: Cyber Security Procurement Language for Control Systems, September 2009

7.3 Key Observations

Discussions with DNOs have clarified the existence of different and perhaps not fully coordinated approaches towards cyber security for operational network management systems within the organisations, as was highlighted as a potential weakness in the CPNI self-assessment tool. One particular observation is that this often means there is no single role which is responsible for cyber security across all elements of the operational network management systems. Should this situation continue as we deploy smart grid solutions, smart grid cyber security management will be an even greater challenge.

Cyber security did not appear to be a strong criterion in the evaluation of LCNF tier 2 project submissions from the DNOs. Ofgem's LCNF tier 2 decision document[9] and the report and recommendations prepared by the LCNF Expert Panel[10] both make minor references to data security in the context of security of customer data, and do not make any specific reference to cyber security in the wider context used within this report.

Cyber security concerns on innovation projects appear to be focused mainly on ensuring that technical solutions are applied, particularly to communications architectures, in order to maintain security. The enduring governance and management aspects of security appear to be less of a concern during these innovation activities. This could lead to the results of innovation projects being used to inform large-scale deployment decisions without proper consideration of how cyber security should be maintained on an ongoing basis. Additionally, security of smart network devices that will be located in the field, and the enduring management of that security, does not appear to feature strongly in DNO activities in this area.

[9] Ofgem - Low Carbon Networks Fund winning projects – Second Tier decision, Ref 147/10, 29 November 2010

[10] Report and Recommendations Prepared for the Gas & Electricity Markets Authority By The Low Carbon Networks Fund Expert Panel, November 2010, Ref 148/10

8 APPENDIX E – NATIONAL GRID

8.1 Digital Risk and Security Consulting

National Grid has a dedicated risk and security consulting team in place which has responsibilities to provide cyber security input to current organisational initiatives and projects. They provide security expertise in terms of strategy, architecture, data protection and regulatory matters. The Digital Risk and Security Consulting team has been expanding in number and capability over the past eighteen months and is headed up by the Chief Information Officer. The team is part of the Information Services function and has capability to utilise a global pool of knowledge and resource including a data protection officer. They also engage with partners and outsource where and when appropriate.

8.1.1 Risk Assessments

An important part of any project or initiative is to establish a baseline set of requirements that satisfy project and organisational objectives. The Digital Risk and Security team typically engage proactively in the initial stages of work to ensure that relevant security aspects are considered at the outset and security requirements are revealed and established. This is a recognised triage phase which is employed. Risk assessment plays a dominate part to expose, quantify and prioritise levels of risk in order to understand and measure potential business impact. No particular risk assessment methodology is mandated by the team, for example IS1, however, this may be used along with other considered methodologies depending on the situation being addressed. Risk assessment activities are recorded and maintained in a risk register.

8.1.2 Governance Arrangements

The Digital Risk and Security consulting team are utilising 27001/27002 as a framework for cyber security guidance; however, there is no formal compliance to this standard. They also utilise NISTIR 7628, other standards and guidelines.

8.1.3 Key Observations

There is a strong body of expertise within the Digital Risk and Security consulting function and this could be extended further and be mutually beneficial through more active engagement and collaboration on specific cyber security matters with other organisations within the industry, in particular, with the distribution network organisations. Engagement with industry wide initiatives should be developed, in particular through organisational cyber security awareness initiatives, process development and smart grid technology deployment. The integration of these components should be considered from a collaborative national perspective industry wide.

9 APPENDIX F - EUROPEAN ACTIVITIES

9.1 European Smart Grids Task Force

The stated mission of this Task Force[11] (TASK FORCE FOR THE IMPLEMENTATION OF SMART GRIDS INTO THE EUROPEAN INTERNAL MARKET) is to advise the Commission on policy and regulatory directions at European level and to coordinate the first steps towards the implementation of Smart Grids under the provision of the Third Energy Package.

The Task Force mission statement also states that it will take stock of technology visions and developments performed by other groupings of stakeholders in this area, including the Smart Grids European Technology Platform, the Smart Grids Forum and the European Electricity Grids Initiative (EEGI), and will be in close contact with their further developments. It also takes into account all the relevant standardisation efforts being undertaken at EU level concerning the functionality, interoperability and standardisation of Smart Meters.

In order to achieve its mission, the Task Force identified three fundamental tasks as follows:

- TASK 1. Produce a common vision in conjunction with institutional actors and key stakeholders for the implementation of Smart Grids;
- TASK 2. Identify the strategic decisions and regulatory recommendations for the EU-wide implementation of Smart Grids;

[11] MISSION for the TASK FORCE FOR THE IMPLEMENTATION OF SMART GRIDS INTO THE EUROPEAN INTERNAL MARKET, adopted by the Steering Committee at its 2nd meeting, held on 16.12.2009

- TASK 3. Produce a strategic roadmap for the implementation of Smart Grids and Smart Meters into the European internal market.

Having defined tasks, the Task Force defined a work programme to be delivered by three Expert Groups (EGs) as follows:

- EG1 – Functionalities of Smart Grid and Smart Meters. This group is tasked with delivering an agreed set of minimum functionalities of Smart Grids and Smart Meters. From the standards perspective, the defined deliverable from EG1 includes recommendations to integrate a standardisation strategy into the overall strategy for Smart Grids, and a definition of the extent of the need for a mandate on Smart Grids standards. Thus, it is expected that EG1 will make recommendations about the strength and depth of Smart Grids standards for Europe;
- EG2 - Regulatory recommendations for data safety, data handling and data protection. From a standards perspective, this group will provide recommendations for standards relating to data security and privacy;
- EG3 - Roles and responsibilities of actors involved in the Smart Grids deployment. From a standards perspective, this group will provide recommendations regarding responsibilities for the development of Smart Grids standards.

9.1.1 EG2 - Regulatory Recommendations for Data Safety, Data Handling and Data Protection

EG2 has documented its activities and recommendations in a final report[12]. The scope of its activities and recommendations are focused mainly on tackling issues such as energy theft and privacy, and the final report cites these as the two most important concerns related to smart grid implementation in Europe. The risk of malevolent attacks is seen to be a risk which is of greater concern outside of Europe. Hence the recommendations made by EG2 are particularly focused on data security and privacy, and do not consider smart grid cyber security from the perspective of smart grids being part of the CNI.

The key recommendations of EG2 are as follows:

- That EG2 should be tasked with further work to assess how privacy and data protection issues of smart metering and smart grids could be addressed. This should consider if this can be achieved within the existing EU privacy and data protection

[12] EG2 Draft Report, Delivered at the 5th Steering Committee Meeting, June 22 2010

framework, or via an additional legal framework, in order to create an EU-wide detailed privacy standard for smart metering and smart grids;

- European Standards Organisations (ESOs) CEN, CENELEC, and ETSI should mandate that smart grid products and solutions should be designed incorporating agreed data privacy and security principles at their core;
- ESOs should be tasked with either updating, extending or developing new standards regarding security aspects of smart grid interfaces based on European requirements;
- That the ESOs joint working group review these EG2 recommendations and relevant documents before starting new standardisation activities;
- ESOs are tasked with evaluating the current state of cryptographic primitives and specify the most appropriate technologies within the relevant technical standards framework. This should include consideration of European level key management;
- All European countries adopt the same generic model for key management, and security and privacy principles;
- Security and privacy principles should be applied to smart meters and other devices in the smart grid if communicating consumption data;
- Data handling should be the subject of further pilot projects, in consultation with other industries such as banking and payment cards. These projects should result in the definition of high level data handling principles for smart grids, which could then be the subject of European standardisation;
- Data privacy should be improved by differentiating between consumer data and technical data, and applying different controls to the different types of data;
- That EG2 should be tasked with further work to define a clear division of roles and responsibilities regarding ownership, possession and access to smart grid data.

9.2 EU directives

The Council of the European Union issued a directive in 2008 which could have some relevance to smart grid cyber security. Directive 2008/114/EC[13] obliges member states to identify potential European Critical Infrastructures (ECIs), which are defined as assets or systems essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, located in member states, where disruption or destruction of these assets or systems would have a significant impact on at least two

[13] COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

member states. Furthermore, the directive obliges members states to inform potentially impacted member states about the existence of ECIs, to inform the owners/operators of the ECI about its designation as an ECI, and to develop Operator Security Plans (OSPs) and appoint Security Liaison Officers (SLOs) for each ECI.

9.3 Key Observations

The scope of the activities and recommendations of the European Smart Grids Task Force Expert Group 2 are focused mainly on tackling issues such as energy theft and privacy. Therefore EG2 does not consider smart grid cyber security from the perspective of smart grids being part of the CNI. This is a major shortcoming in the work of EG2, and highlights a significant difference in focus between UK activities and European activities, especially given that the risk assessment undertaken by the SMIP with respect to GB smart metering has identified high priority risks which are due to smart metering being part of the CNI.

Whilst it is believed that smart grid developments in the UK are unlikely to be defined as ECIs in the main, it is not impossible that key smart grid deployments and future cross border interconnections could become mutually dependent. This could result in smart grid deployments being defined as ECIs and therefore subject to EU directive 2008/114/EC.

10 APPENDIX G - INTERNATIONAL STANDARDS AND GUIDELINES FOR SMART GRID CYBER SECURITY

This section summarises a review carried out on the NISTIR 7628 Guidelines for Cyber Security, in particular to establish its applicability to form part of a framework for Cyber security in the UK. In addition the material and attributes of some relevant ISO/IEC and ANSI standards were also considered with the same objective in mind. Current literature and reports commenting on these standards and their applicability to smart grid cyber security were also part of this work. This study is not intended to be a detailed analysis of specific standards however, it yields the information required to understand the purpose of the material and the applicability of NISTIR 7628 and other standards reviewed in the context of a UK framework for smart grid cyber security.

10.1 NISTIR 7628

This section provides a brief introduction of the National Institute of Standards Interagency Report, NISTIR 7628 „Guidelines for Smart Grid Cyber Security", giving an overview of its origin, purpose and applicability to the development of a smart grid cyber security strategy and framework in the UK. For convenience 13has a brief description of the chapters and appendices of all three volumes of NISTIR 7628.

The development of the NISTIR 7628 Guidelines is a relatively large scale focused development involving several diverse organisations and groups. The initiative was driven by Congress through the Energy Independence and Security (EISA) Act 2007 with a key objective to support Smart Grid Security as a National goal. From this, NIST was assigned "primary responsibility to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of Smart Grid devices and systems…" The decision origin, flow and the appointed groups tasked to address this objective are shown in Figure 8 - The Origin of the National Policy.

.

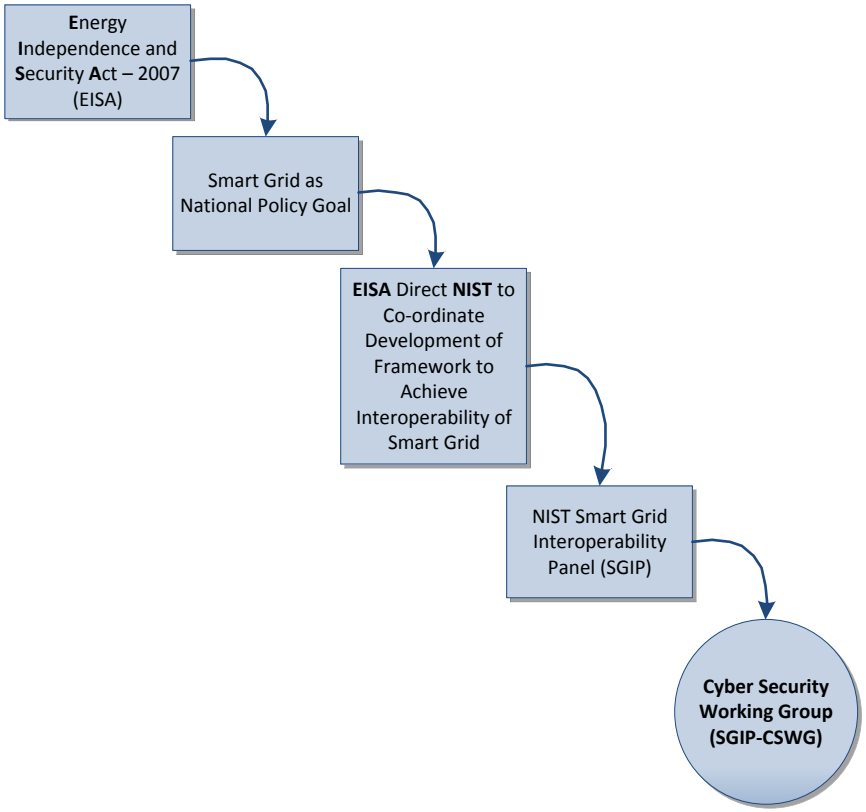

Figure 8 - The Origin of the National Policy

10.1.1 Smart Grid Interoperability

Notice from that first and foremost there is a Policy driving this initiative. From this, NIST have an objective to develop a Framework that will achieve Smart Grid Interoperability. To put the word „interoperability" in context for the purposes of this report, the concept exhibits the features of a multi-layered architecture with many interdependent technical and organisational boundaries. For example, consider the simple case of the technical functionality required to establish communication between two networked devices from different vendors. Both vendors will have to agree, conform and implement the protocol requirements to achieve successful communication. As another example, consider the case where data or information is passed from one part of a system or organisation to another, additionally, with an essential change of ownership and accountability for the data or information. In this case, this is a decision that has to be agreed up-front as policy and

agreed by appropriate management on both sides. To resolve it may require deployment of new technology, appropriate process, regulatory controls or legal agreement. The main point here is that to achieve interoperability, all of the associated technical components, systems and organisational aspects must be considered. It is an organisational level requirement that has to be agreed through policy with the appropriate level of management, the involved parties and deployed into a suitable architecture assuring end to end reliability with cyber security in mind.

10.1.2 **Cyber Security Working Group (SGIP-CSWG)**

As part of the Smart Grid Interoperability Panel (SGIP), the Cyber Security Working Group had the responsibility for engaging and co-ordinating the contributions from all participants and for the timely delivery of the Guidelines. The development of this work has been on-going for some years but was particularly intense for a 17 month period prior to the August 2010, V1.0 release. NISTIR 7628 is a result of co-operative and collaborative effort which has captured an extensive amount of cyber security knowledge from around 475 participants through its development resulting in many man years of work. Participants and contributors include US government agencies, regulatory bodies, academia, various industry vendors and representatives, public and private groups, including interested individual contributors. The structure of the collaborative approach by the working group and an example of some of the participants are illustrated in Figure 9-The Cyber Security Working Group.

.

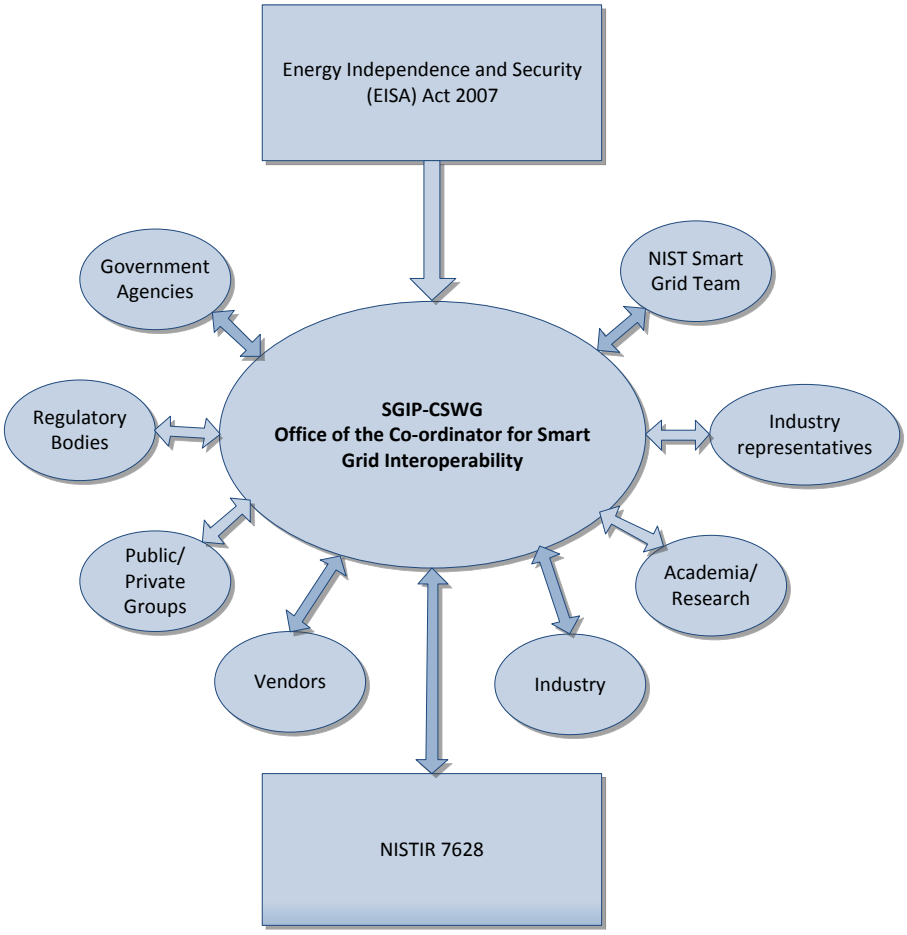

Figure 9-The Cyber Security Working Group

10.1.3 NIST- CSWG Standards Review

As part of coordinating the development of a framework that includes protocols and model standards for information management to achieve interoperability, the CSWG had an additional sizeable task. Through the Energy Independence and Security Act of 2007 (EISA), the CSWG were tasked with carrying out a „Standards" Review. To manage this activity the CSWG set up a „Standards Sub Group".

This involved an assessment of the 75 standards listed in the Special Publication document „NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0". The objective here was to review the standards against the requirements defined in NISTIR 7628 and produce a summary of standards which were identified and applicable to Smart Grid. In

other words the NISTIR 7628 material was used as a reference to establish the applicability of the respective standards identified. During this process the standards were assessed for requirements coverage, including gap analysis identifying additions and amendments, resulting in the list given in Table 4.1, Section 4.2 of the Framework and Roadmap document. Figure 10 – Standards Review Activities illustrates the activities carried out by the CSWG Sub-Group during the Standards review.

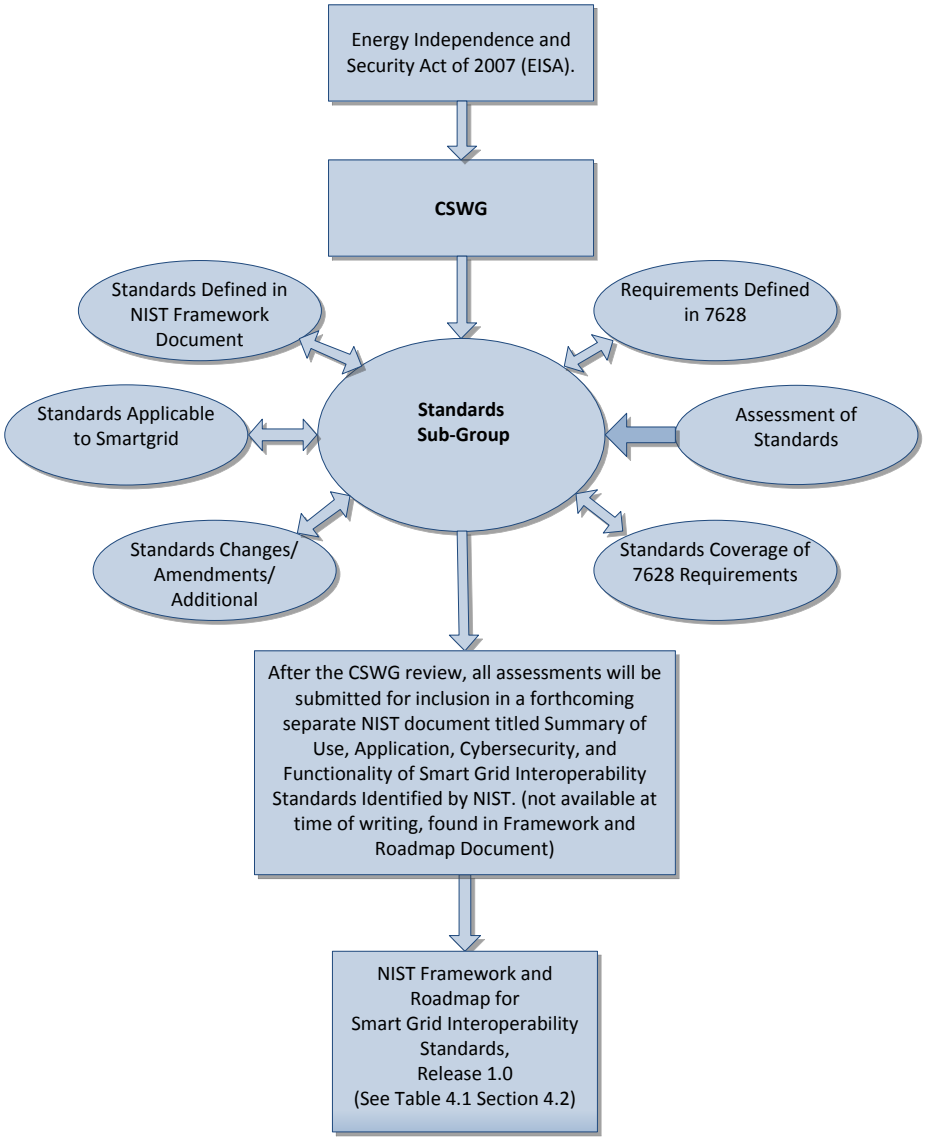

Figure 10 – Standards Review Activities

10.1.4 The Government Accountability Office Report (GAO-11-117) on NIST

The Government Accountability Office (GAO), are an independent investigative arm of congress and were recently tasked with carrying out an assessment on NIST activities with regard to the development of cyber security guidelines. They published a report in January 2011 of the assessment and there were some interesting findings. For example, The EISA does not provide the Federal Energy Regulatory Commission (FERC) with enforcement authority and therefore oversight of interoperability standards is not mandatory in any sense,

and effectively, the deployment of cyber security controls remains voluntary. However, this has been acknowledged and an agreement between NIST and FERC that „FERC develop a coordinated approach to monitor voluntary standards and address any gaps in compliance". Another interesting point is that there is no forum or process in place to share cyber security information and also no evidence of measurement and metrics to quantify the effectiveness of the controls. In conclusion, it seems benefit could be gained by utilising the guidelines material selectively as part of a structured operational and cyber security management system.

10.1.5 **Utilities Telecom Council – Information Bulletin Published 25th August 2010**

This document was prepared and published by the Utilities Telecom Council Public Policy Division. A prominent objective of this report is to provide some high level recommendations extracted from the content of the NISTIR report to help utility organisations plan for their specific security needs in order to prepare and ensure future regulatory compliance. It is clear from the report that NISTIR 7628 will have a strong influence and impact on cyber security and regulatory matters.

It points out some of the regulatory difficulties dealing with current and future Smartgrid considerations, for example, regarding interoperability, standards and policies and it also makes some comment on the technology and business model challenges facing existing systems. Currently there is no clear regulatory structure to provide clear mandates to establish the best protection for current and next generation Smartgrid systems and it is also observed by the authors that there are no „how to" guidelines for utilities to address existing and next generation systems.

It references eight Critical National Infrastructure Protection reliability standards (NERC CIP 002-009) used to protect national systems against potential cyber security breaches. NERC CIP 002 considers specifically critical cyber assets. These standards were FERC approved in 2008.

In a practical sense there is valuable comment on how to approach addressing cyber security. It picks up on an important point from NISTIR about how to start breaking down the systems into manageable chunks that can be categorised and reviewed with robust functionality and cybersecurity in mind. Another interesting point made was for utilities to ensure that vendors provide compliant solutions.

It mentions for the future that process should be developed and deployed and organisations should establish a practical cybersecurity strategy ensuring risk assessment plays a key part. In the „Next Steps" section of the document, point „f", it comments on „people, process and technology", however, there is limited comment on the „people" side. This is fairly common in most approaches to addressing cyber security but it should be clear that the people, organisation structure, roles and responsibilities are key to a successful cyber security management strategy.

10.2 **ANSI/ISA-99 / IEC-62443**

In terms of security, the general purpose of standards is to provide the organisation with a structure and framework of controls that will protect organisational assets from harm on a continuous basis, for example, from internal security breaches, such as human or electronic protocol violations and of course malicious cyber-attacks. The standards employed must accommodate and align with the operational environment and be tailored to meet the organisation's top level security policy requirements.

ANSI/ISA-99.02.01-2009 is a standard for "Security for Industrial Automation and Control Systems (IACS): Establishing an Industrial Automation and Control Systems Security Program." This standard is tailored to IACS, where in addition to normal IT or information security considerations there are health and in particular safety issues to be considered in parallel with security. In short this standard provides guidance on policy, procedure and practice on how to develop the elements and controls required establishing a Cyber Security Management System for Industrial Automation and Control Systems. ISA is predominantly a US-focused organisation, and in an effort to reach a broader audience and have more visibility in Europe, ISA collaborated with IEC on this work and ISA99.02.01-2009 is now approved and published by the IEC as 62443-2-1 in November 2010.

There is a current on-going development to adjust this standard to align more closely with the ISO/IEC 27000 family of standards and ISA have committed to completing this work by the end of 2012. A new version is expected to be complete by the end of 2011 to account for IEC review, voting and publication time-frame. These, along with the 27000 family, are strong candidates as a starting point for a framework which is appropriate for the UK.

10.3 ISO/IEC 27001/27002

This standard formally specifies an information security management system framework to bring information security under the explicit control of management. This is a formal specification and it mandates specific requirements, so a formal auditing process is required to be certified to this standard. The point here is not about the certification process but more about having the management framework in place with ownership and accountability for security. However, formal compliance encourages a level of governance and expectation across the board. It encourages common practices and yields benefits from sharing best practices.

It is a „risk" based management system and specifies the overarching structural requirements which define the information management framework, including guidance to deploy, monitor and continuously improve the system. It is conveniently flexible, in that it does not mandate specific information security controls, in other words there is flexibility for the organisation to implement and deploy specific controls and practices which can be tailored to meet the operational environment security requirements of specific system assets and functions.

10.3.1 ISO/IEC 27002

This is the code of practice for ISO/IEC 27001 which are guidelines used to help construct the management system and meet the requirements stated in ISO/IEC 27001. Not all of the controls and guidance in the code of practice may be applicable to the organisation. There is flexibility here, for example, additional controls and guidelines not included in this standard may be required and legitimately used. There is a mandated „Statement of Applicability" which is required. This is an up-front statement of what sections of the standard the organisation intends to comply with and what it intends not to comply with giving reasons why in both cases. This again adds some flexibility and more importantly a top down approach to developing a framework.

10.4 Key Observations and Recommendations

In some literature and by some in the cyber security community NISTIR 7628 is loosely referred to as a „Standard" which in itself may imply an association with some level of regulatory compliance, mandatory or otherwise. This is not the case or intention of 7628. The volumes of the document are very comprehensive and wide ranging; however, it is not

formally accredited as an approved or certified regulatory standard in the United States, for example, like some ISO/IEC standards which have formal accreditation through UKAS in the UK. The Guidelines are not prescriptive as you would expect from a standard, nor are they mandatory. They are advisory, intended to facilitate and compliment efforts to develop smart grid cyber security practices and controls effectively.

The Guidelines extend to facilitate specific domain requirements and use case scenarios which can be used to assist developing a practice, control, standard or form part of a framework to improve operational security. It is an impressive collection of knowledge and a good source and reference point for addressing and developing domain specific cyber security practices. However, they are not suitable to be adopted as a structured regulatory framework as it stands, but should be used selectively to assist in the development of cyber security requirements.

Although the material is extensive and detailed there is little guidance on where to start with regard to prioritising and developing a strategy to put an effective smart grid cyber security management system in place. NISTIR 7628 is therefore best considered for use in later stages of work when specific cyber security risk assessments have been carried out and potential vulnerabilities have been identified. It is more aligned to a bottom up approach.

At this stage, and as a starting point for the development of a smart grid cyber security framework for UK application, it would seem most beneficial to take a top down approach. An overall smart grid risk assessment at national level will help develop an understanding of the prospective scope of smart grids, and will assess security risks at this high level. The results of this approach could then drive further more detailed activities at DNO level. At this level a blend of the standards discussed previously is most likely to prevail to develop aligned policies, procedures, framework structure and controls. For example, using ISO/IEC 27001 requirements, and the ISO/IEC 27002 guidelines to start establishing and developing a smart grid cyber security framework. The CPNI Good Practice Guidelines and ISA 99 / IEC 62443 series could be used to help develop the operational practices and controls along with selective use of the NISTIR Guidelines to address specific security scenarios and low level asset specification and conformance controls.

11 APPENDIX H - NATIONAL LEVEL SMART GRID CYBER SECURITY FRAMEWORK

Whilst smart grids may not be delivered via a national rollout programme in the UK, the resultant architecture and the operation of it will clearly be CNI. It is therefore important to understand the prospective scope of smart grids at a national level, and to assess security risks at this high level. This will help identify key security risks for a generic UK smart grid architecture, and could be used to assist the organisations actually deploying smart grids (i.e. the DNOs) in understanding the key risks that need to be managed as part of their smart grid deployment projects and operations.

11.1 Risk Assessment

In order to understand the prospective scope of smart grids at a national level, and to assess security risks at this high level, the IS1 methodology is proposed. There are clear benefits to using this approach, which include:

- The methodology is mandated for Government systems and is therefore a well-established and mature methodology;
- Necessary skills already exist to some extent within the UK electricity industry, due to its use by the Smart Metering Implementation Programme.

This section presents the progress that has been made to date using this approach.

11.1.1 Catalogue of Assets and Foci of Interest

In line with steps 1 and 3 of the IS1 approach, a catalogue of assets, grouped into Foci of Interest, has been identified. This was based on certain aspects of smart grids for the UK which are already well known and established, plus certain aspects of smart grids that are not currently implemented. Those aspects that are not currently implemented consist of emerging technologies and evolving systems, some of which are the subject of pilot projects by UK or international electricity network companies, for example as part of IFI or LCNF funded projects, and some of which we envisage will become available at some point in the future. It should therefore be noted that the assets presented in this section are an initial

view, and should be subject to regular review and update at smart grid technologies evolve and new systems are implemented.

The assets were built up using a number of sources. Firstly, the assets identified by the Smart Metering Implementation Programme were added in order to incorporate the smart metering element of smart grids, whilst retaining alignment with the Smart Metering Implementation Programme itself. The assets are therefore as illustrated in Figure 6.

Next, a representation of the typical arrangements for existing electricity network management systems was added. These are the systems in place today and used by the electricity network companies to monitor and control the networks. In terms of cyber security, these are the systems that the electricity network companies currently focus their cyber security efforts on. Figure 11 below illustrates these assets, where SCADA/DMS identifies central control and monitoring systems (Supervisory Control and Data Acquisition/Distribution Management Systems), usually located in physically secure control centres. From the SCADA/DMS, control and monitoring at various points on the network is possible, via substations and other electrical assets on the network which can communicate with the SCADA/DMS. In older systems, communications use proprietary protocols over low bandwidth communication media such as radio, microwave, dial-up PSTN or leased line telecommunications. More modern systems use open standard protocols over higher bandwidth communication media including mobile telecommunications technologies such as GPRS.

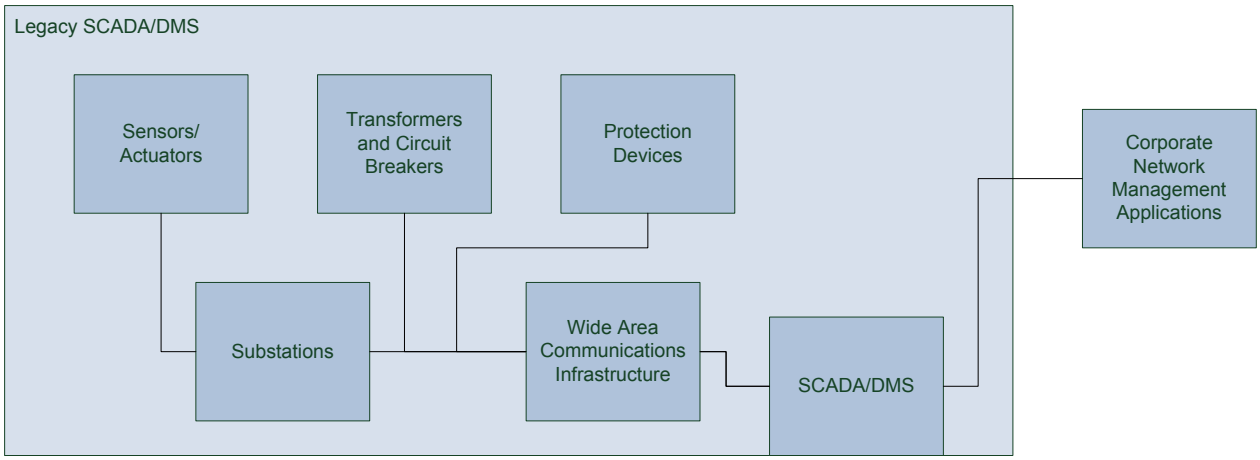

Figure 11 - Legacy SCADA/DMS Assets for Risk Assessment

Finally, a representation of the anticipated arrangements for future smart grid management systems was added. As noted above, this was based on emerging and evolving

technologies as well as already available smart grid solutions. Figure 12 below illustrates these assets. Much of the assets will be modern equivalents of the legacy arrangements described above, however the communications between them will be based on open standard protocols over high bandwidth communication media. The open standard protocols are likely to be based on routable protocols (IP-based) compared to the point-to-point protocols primarily used in the legacy arrangements. There are also two additional types of assets which are anticipated to be present in the smart grid. These are as follows:

- Smart appliances. These will be end devices which are monitored and controlled directly by the electricity network companies, rather than via the smart metering infrastructure. This means that they are unlikely to be domestic smart appliances in the home, but could be larger commercial or industrial smart appliances such as refrigeration units, building management systems or larger scale smart charging systems for electric vehicles.
- Smart grid network controllers. These will be controllers for autonomous management of localised portions of the smart grid, for example to manage constraints or to actively manage power flows at a local level. Whilst these devices may operate autonomously, they will also have to communicate and coordinate with adjacent network controllers, and also with central smart grid SCADA/DMS systems.

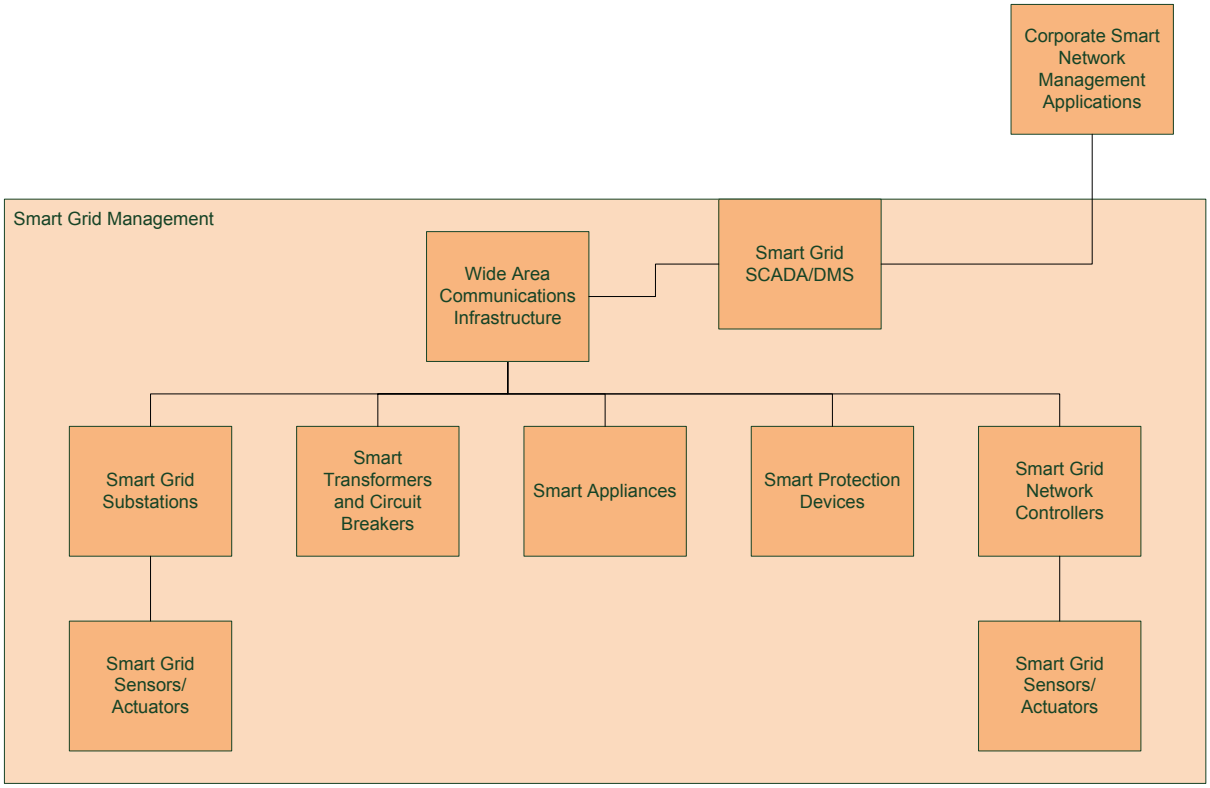

Figure 12 – Smart Grid Management Assets for Risk Assessment

Using these three sources, an overall picture of smart grid assets are built up for the purposes of risk assessment. The overall picture also recognises the dependencies that will exist between the sets of assets in order to facilitate a comprehensive smart grid. This is illustrated in Figure 13 below.

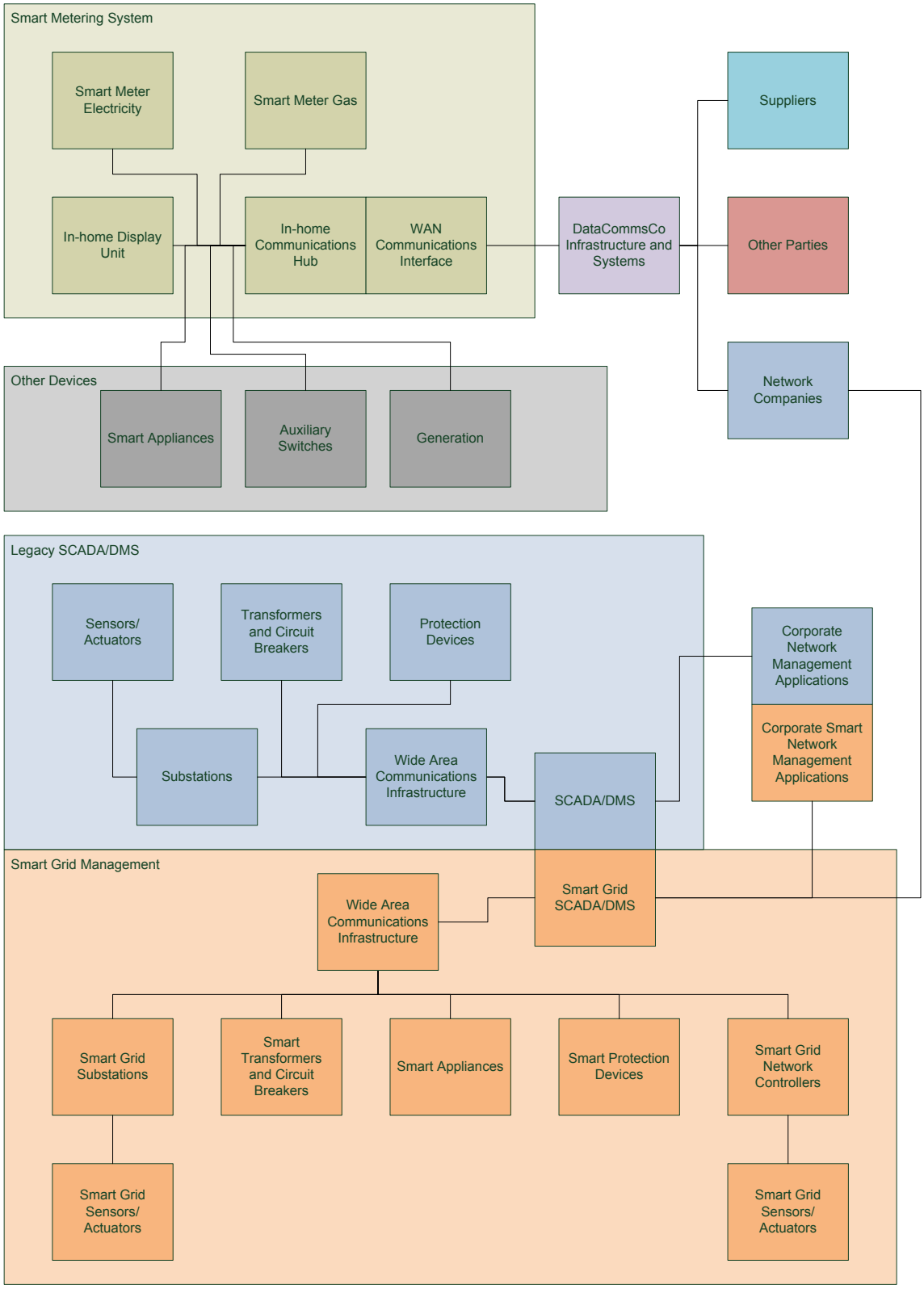

Figure 13 – Overall Smart Grid Assets for Risk Assessment

11.1.2 **Subsequent stages of IS1**

Other stages of IS1 are:

- Identify and Assess Threat Sources and Actors;
- Calculate Risk Levels;
- Prioritise Risks.

The IS1 risk assessment undertaken by Ofgem on the SMIP has been an ongoing activity since September 2010, and is due another iteration in March 2011 as a result of feedback from the STEG. Comparing the scope of the IS1 effort on the SMIP with the scope of any IS1 effort for smart grids, we can see by comparing Figure 13 with Figure 6 that the scope of smart grids is very much greater and therefore the effort required will be significantly greater than that required for the SMIP.

11.2 **Key Observations and Recommendations**

11.2.1 **Risk Assessment**

The work already completed on smart metering risk assessment using IS1 could provide valuable input to any smart grids risk assessment work. For example, threat sources and threat actors could be similar for both smart metering and smart grids, although the list of smart grid threat actors would need to be expanded to include for example DNO communications infrastructure users, DNO field installation and maintenance personnel, and privileged DNO control centre personnel. It should be noted that the results of the smart metering risk assessment are classified, so they cannot be detailed or discussed in this report, and would need to be obtained through an appropriate channel and authorised for use for smart grids risk assessment.

Completing and subsequently maintaining a smart grids risk assessment at national level using IS1 would allow DECC to develop and maintain an overview of the key smart grids risks, which could then be used to drive/steer DNO security related activities. It should be noted that we are not recommending that this would be the DNOs only source of risk information, as each DNO should also be expected to identify other risks specific to their own situations, and also seek to address those risks.

Risk assessment activity at this level could be completed in consultation with CPNI and CESG, as has been done with the smart metering risk assessment.

It should be noted that the IS1 standard is focused on technical risk assessment, meaning that it excludes non-technical risks such as physical risks and natural disasters. However, care should be taken that this does not narrow the focus of risk assessment too much; for example, risks due to the actions of persons interacting with the system as users (authorised or otherwise) must also be considered.

It should also be noted that IS1is an Information Assurance standard and is therefore strictly limited to (information) security; other risk assessment activities should consider the other aspects of dependability i.e., reliability, safety and maintainability.

Through the work done to date in reviewing DNO approaches to cyber security for current operational systems and also for pilot smart grid solutions, we believe that a number of key risks are evident. These risks should be further explored as part of a more detailed risk assessment. The risks are:

- Security in design, installation and management of devices in the field, which in the future will be smart grid devices. Security considerations in the design, installation and management processes are less evident for devices in the field than they are for centralised services such as wide area communications and SCADA systems;
- Security governance of current operational systems end-to-end (i.e., from control centre to the end measurement or control points on the network), and therefore security governance of smart grid end-to-end. The key area of risk again appears to be around field devices;
- Consistency, breadth and depth of security risk assessment within the DNOs. Inconsistent approaches can lead to differences in calculated risk levels and inconsistent treatment of risks. Risk assessment is often undertaken in a generic sense, but doesn't consider specific cyber security risks, especially for equipment that is not considered IT equipment;
- Third party risks. DNOs are highly dependant on third party suppliers and service providers. As with security governance, third party risks are not always considered from end-to-end within current operational systems, and therefore the same applies to smart grids.

11.2.2 **Government/Regulatory Activities**

In addition to the risk assessment recommendations above, and building on the observations in section 6.5, government and/or regulatory activities should ensure that:

- The Smart Grids Forum incorporates consideration of smart grid cyber security into its work, from the perspective that smart grid cyber security requirements will need to be established and satisfied in order to help manage risks to security of supply;
- One specific area that the Smart Grids Forum should investigate is how to deliver coordinated smart grid cyber security efforts across all stakeholders. This could entail some level of security management or coordination at national level, and possibly the setting of some expectations (or even more strict obligations) on the DNOs for how they approach smart grid cyber security and how they report on it;
- The DNOs approaches to smart grid cyber security on LCNF project bids should be considered as part of the evaluation process, explicitly examining how the DNOs plan to deliver continued security of supply should the new smart grid technologies being trialled suffer cyber security vulnerabilities at any point in their lifecycle after deployment;
- CPNI reviews its good practice guides and self assessment approach with particular focus on requirements for smart grid cyber security.

12 APPENDIX I - ORGANISATION LEVEL SMART GRID CYBER SECURITY FRAMEWORK

12.1 Organisational and Cultural Adjustments

It is common in some organisations that cyber security is assumed to be the sole responsibility of the IT function. However, addressing cyber security requires attention and commitment from all employees within an organisation including third parties such as vendors, suppliers and contractors engaged temporarily or otherwise with the organisation.

General awareness of security issues of various types and at various levels is becoming more commonplace. For example, awareness of security concerns ranging from national terrorism threats through to fraud/theft is increasing, all of which are constantly changing in form and becoming more of a concern as public and personal threats. This has naturally heightened public sensitivities and there is an expectation for people to be more vigilant, and to report suspicious circumstances and incidents to the appropriate authorities. In a public sense, this responsibility is now accepted and practiced on a daily basis. To better address cyber security issues in industry, this mind-set should be extended into job roles as accepted working practice on a daily basis. The same principles of awareness, vigilance and responsibility must be communicated throughout the organisation and practiced as a matter of course.

It is expected that as organisations adjust to accommodate new smart grid technologies it should be clear that there will be new and additional responsibilities concerning cyber security within the workplace and in many cases this will require some cultural and mind-set adjustments. Cyber security should be considered as an inclusive and integrated element of job function driven by policy from the top of the organisation through to field operations.

12.1.1 The Current Role of the Corporate IT Function

Managing cyber security is commonly perceived to be the responsibility of the organisation's Information Technology function, usually involving the deployment of familiar hardware, such as network firewalls, switches and routers. Generally speaking, these components are

understood to secure network topology, servers, PCs, mobile devices and utilities which form part of the organisation's critical operational infrastructure. The IT function also has a strong association with the deployment and administrative support of preventative and defensive software packages such as antivirus, anti-malware and cryptographic applications to secure and protect data in transit and mobile communication devices.

In most if not all IT deployment situations we have to consider and manage a level of risk on a dynamic basis to provide a safe, secure and convenient operational platform with a convenient level of access for users which supports productivity and essentially provides or enables business continuity when disruptive events prevail or security incidents occur. IT is of course an essential part of our corporate infrastructure and will remain so and develop as an essential function in our cyber security strategy. This requires engagement in continuous improvement strategy, considering and employing evolving technologies which can play a key part in improving the security of our critical infrastructure and day to day operations.

It is clear that IT functions in organisations already have extensive experience managing systems and cyber security issues, not just in a technical sense, but from an overall IT governance perspective. It is important to utilise and build on this available experience and knowledge. To address the cyber security challenges currently anticipated it is essential to identify and extend asset and functional ownership for cyber security throughout all functions and levels of the organisation. Accountability for cyber security should be realised as an integral part of all job functions within the organisation from the top down and will require a more integrated cross functional co-operative and collaborative approach.

The remainder of this section outlines a proposed framework for the management of cyber security within the DNOs.

12.2 Smart Grid Cyber Security Management Framework

Improved cyber security requires engagement, collaboration and co-operation of all parties within the DNO and including external third parties. The framework and structure presented in this section proposes a security strategy which addresses cyber security from an organisational point of view. This requires a defined cyber security policy, driven and enforced by top management, including appointed ownership and accountability through all managerial levels to operations. Active and continuous lifecycle engagement is required by all parties throughout the organisation. Ultimate responsibility for cyber security in the organisation lies of course with management, however, the effectiveness of applied controls

and implementation lies within business operations with the staff. This section describes the key elements appropriate for a Smart Grid Cyber Security Framework within the DNOs. In order to encompass an overall approach to security for DNOs, we have used a more generic title of Operational Security Management System (OSMS), as presented in Figure 14 below.

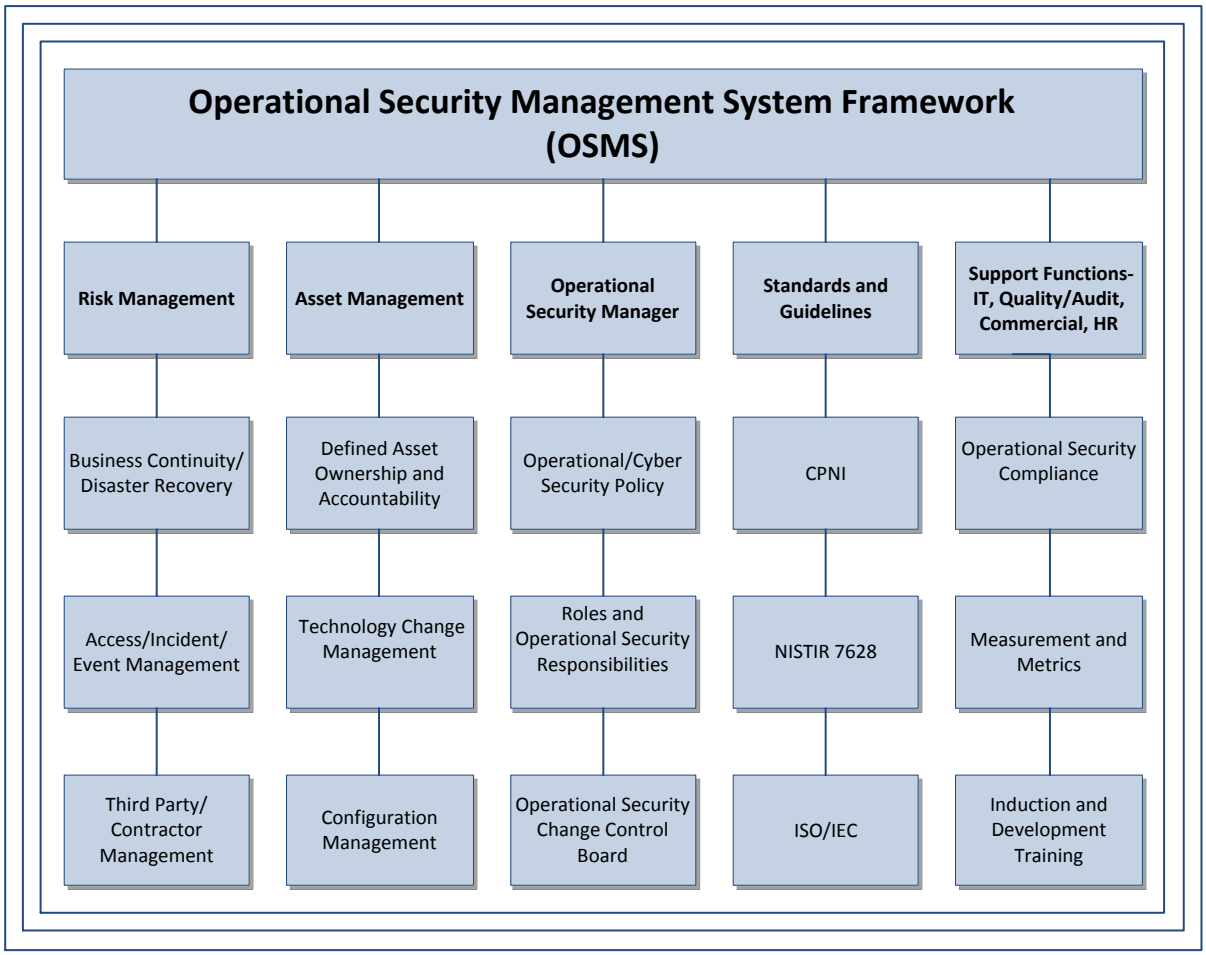

Figure 14 – OSMS Framework

This framework captures some of the key activities that will be required in the OSMS and should be tailored and enforced through policy following a proper detailed audit of a candidate DNO. The Structure of the OSMS Framework, for management purposes, is broadly aligned with ISO 27001 requirements and depicts some of the elements that should be considered by DNOs. There is flexibility to include controls or practices from other sources, in this case we would expect to utilise the CPNI guidelines and other applicable standards and guidelines as appropriate to address lower level cyber security considerations. This level of detail should be considered following detailed audit and risk analysis.

We believe that most of the functions and terms in the framework are fairly familiar and well understood in the industry. However, one key area is the deployment of a Technology Change Management strategy, which should be employed to address moving from legacy technology to smart grid technologies.

12.2.1 **Smart Grid Technology Change Management Control**

As the smart grid is developed there will be a demanding need to evaluate new technologies and tools, new controls, practices and prepare associated training programmes. Replacing, superseding or introducing new technologies, devices, tools or equipment carries a level of risk through procurement, deployment and operation. This is the case now and will continue to be so with more challenges for smart grid technologies. The main demands placed on legacy technology and equipment are of course to be dependable, functionally reliable, physically and electrically robust and be cost effective. There is an added dimension to this specification for smart grid in that, they now need to be operationally secure in real time and provide continuity of service in the face of potential disruption, whether this be malicious, fraudulent, environmental or from other threat sources.

As part of the cyber security framework, technology changes should be deployed through a controlled lifecycle of Smart Grid Technology Change Management controls. This is a pro-active scalable practice that can complement current methods and help control and reduce operational risk. The Technology Change Management lifecycle begins in the early stages of change request through requirements capture and procurement to retirement of the technology cost effectively. The following strategy defines the main components of what may be considered for a generic Technology Change Management lifecycle including how it is controlled and facilitated. The scope of the lifecycle considers and includes management of commercial off-the-shelf equipment and technologies. However, it can be applied to proprietary or customised technologies and in-house developed components and tools.

12.2.2 **Roles and Responsibilities**

12.2.2.1 Operational Technology Change Control Board (OTCCB)

This is an appointed management group which consists of stakeholders within the organisation that have dependencies in operational security matters. As well as the obvious engineering and IT representation it may also include representation from the commercial/finance and Quality function. This should be chaired by the Operational Security Manager.

12.2.2.2 Operational Security Manager

The Operational Security Manager has a defined role with ownership and accountability for the security aspects of Technology Change Management. This role requires upholding the organisation's operational security policies and providing the necessary procedures, guidance and controls to do so. This includes providing the authorisation which controls secure progress through the selected phases of the Technology Change Management lifecycle in line with business requirements and strategy.

12.2.3 **Operational Security Roadmap**

The Operational Security Manager will own, develop and maintain a roadmap of the organisation's cyber security strategy and proactively plan scheduled reviews of current operational assets and functions. This should consider new technology options, further development of existing technology and plans to retire legacy or vulnerable technology on a continuous improvement basis.

12.2.4 **Technology Change Management Lifecycle**

The following diagram, Figure 15 – Technology Change Management Lifecycle , illustrates the lifecycle employed after a Technology Change requirement has been identified and formal change request is submitted to the Operational Security Change Control Board (OSCCB). Following acceptance, OSCCB authorisation is required to proceed to an agreed

phase of the lifecycle. Each phase may be used in isolation or as a sequential part of the life cycle. The Technology Change Management Lifecycle described here is intentionally generic and would be adjusted and tailored to align with the requirements of a specific organisation.

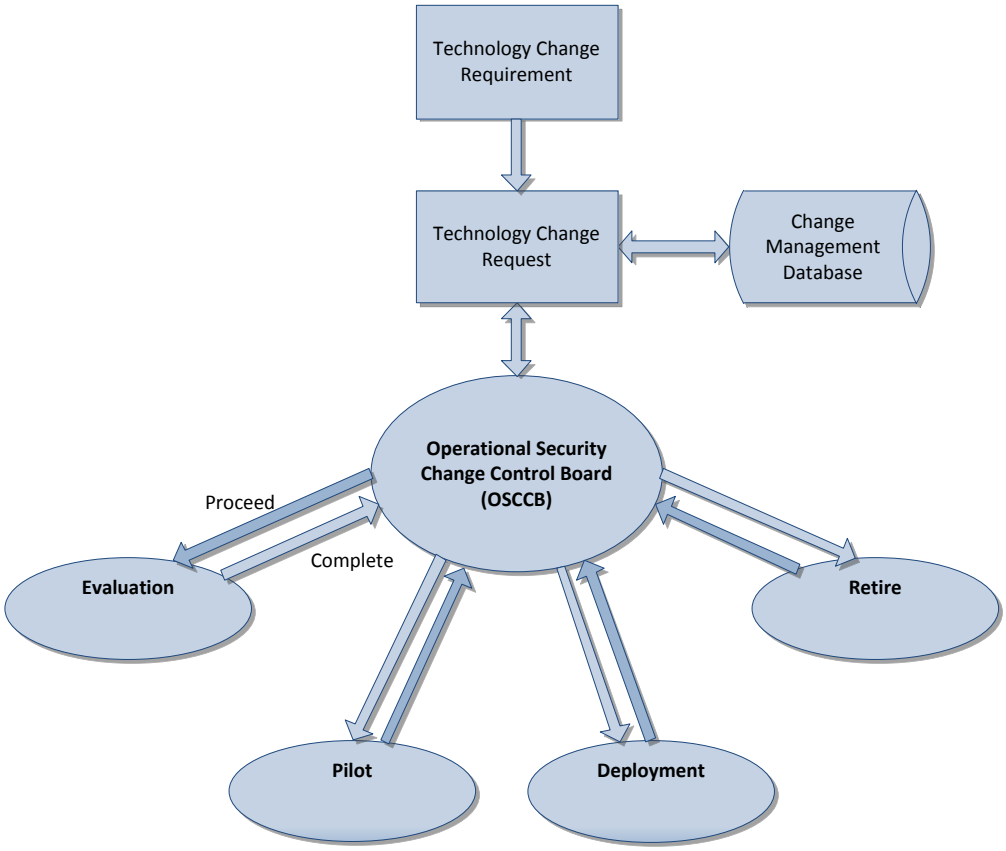

Figure 15 – Technology Change Management Lifecycle

12.2.4.1 Evaluation Phase

This phase is used to consider and select potential candidate technologies that can best satisfy the technology change requirement. The evaluation activities include a risk assessment and cost/benefit analysis of a proposed new technology or development of existing technology. Any identified or selected technology that is potentially a candidate for deployment into the systems must be evaluated to ensure operational compliance with the security requirements or standards defined in the technology change requirements specification. The evaluation phase Inputs, Tasks and Outputs, are defined as follows:

- Inputs
    - Technology Change Request formally accepted by the Operational Security Change Control Board.
    - Operational Security Change Control Board approval to proceed with the evaluation.
- Tasks
    - Risk assessment of the Technology, engaging all affected and potentially affected parties in the organisation and third parties out with.
    - Cost/benefit analysis of new technologies or of existing technology, including integration, maintenance and training considerations.
    - Evaluate the technology for purpose against the pre-defined operational security requirements.
    - Establish comparison and measurement criteria which quantify the level of success or failure of the evaluation.
- Outputs
    - Risk assessment results.
    - Cost/benefit conclusions of the evaluation.
    - Evaluation results of compared technologies.
    - Recommendations to the Operational Security Change Control Board.
    - Authorisation from the Operational Security Change Control Board to proceed to the next step in the lifecycle or to terminate further activity.

12.2.4.2 Pilot Phase

This phase is a controlled exercise which allows for functional and operational security issues to be exposed, identified and addressed up-front with reduced risk, essentially providing information, data and measurement that can aid deployment considerations and decisions. The piloting process is typically used in a low risk operational environment to exercise a controlled deployment of the technology. Candidate sites/systems/equipment and resource will be identified and used as a vehicle to establish the capabilities, performance and suitability of the technology to meet the identified operational security requirements. The evaluation phase Inputs, Tasks and Outputs, are defined as follows:

- Inputs
    - Operational Security Change Control Board approval to proceed with the pilot.
- Tasks

    - Deployment of the technology/systems/equipment and resource at the candidate site/controlled environment.
    - Run the pilot exercise in line with the Operational Security Policy.
    - Extract the key performance indicators, results and quantitative measurement that can aid the Operational Security Change Control Board deployment decision.
- Outputs
    - Pilot results, including conclusions and recommendations to the Operational Technology Change Control Board.
    - On-going maintainability and manageability from a security perspective.
    - Authorisation from the Operational Security Change Control Board to proceed to the next step in the lifecycle or to terminate further activity.

12.2.4.3 Deployment Phase

In this phase the new or developed existing technology will go through a controlled roll-out and be deployed into active service. The deployment phase Inputs, Tasks and Outputs, are defined as follows:

- Inputs
    - Operational Security Change Control Board approval to proceed with the deployment.
- Tasks
    - Prepare deployment plans and schedule.
    - Prepare and deliver training package to affected parties.
    - Communicate deployment plans and expectations to the affected parties within the organisation and third parties out with.
    - Deploy the new technology or existing technology development across the organisation in line with relevant procedures.
    - Update Asset Register.
- Outputs
    - New technology or existing technology development deployed into active service.
    - A report of deployment activities conclusions and recommendations to the Operational Security Change Control Board.
    - Operational Security Change Control Board approval to close technology change request.

12.2.4.4 Retirement Phase

This phase facilitates retirement of a technology from active service. If the technology is becoming vulnerable and is no longer doing the job required, is inefficient and/or not cost effective it should be considered for retirement. This may be evident through a security event or unacceptable frequency of security incidents, normal use, or from a planned review of the technology scheduled on the roadmap; in any case the retirement process will be initiated by a Technology Change Request. The Retirement phase Inputs, Tasks and Outputs, are defined as follows:

- Inputs
    - Technology retirement Change Request accepted by the Operational Security Change Control Board.
    - Operational Security Change Control Board approval to proceed with the retirement of the technology.
- Tasks
    - Prepare technology retirement plans.
    - Communicate retirement plans and expectations to the organisation.
    - Retire the technology from the organisation in line with relevant procedures.
- Outputs
    - A report of the retirement activities including conclusions and recommendations to the Operational Technology Change Control Board.
    - Update the Asset Register.
    - Operational Security Change Control Board approval to close technology change request.

12.3 **Key Observations and Recommendations**

In comparing the approach presented in this section with DNOs current activities, it is likely that in general terms the DNOs are following approaches that are not dissimilar to those presented here. For example, the pilot phase of the Technology Change Management Lifecycle is similar to the pilot projects that the DNOs are delivering under the LCNF and as part of other initiatives. The key difference in the proposed approach presented here is that it includes explicit consideration of operational security in a way that does not appear to be so prevalent in the DNOs current pilot projects.

Adoption by the DNOs of a structured approach such as the framework presented in this section would enable a more consistent and managed approach towards smart grid cyber security, whether as part of new technology pilots or full deployment of smart grid solutions.

13 APPENDIX J - NISTIR 7628 SUMMARY

This 7628 report was developed by members of the Smart Grid Interoperability Panel–Cyber Security Working Group (SGIP-CSWG), the Cyber Security Coordination Task Group (CSCTG).

NISTIR 7628 - Vol 1
Guidelines for Smart Grid Cyber Security:
Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements
The Smart Grid Interoperability Panel – Cyber Security Working Group,
August 2010.

Chapter 1 – Cyber Security Strategy includes background information on the Smart Grid and the importance of cyber security in ensuring the reliability of the grid and the confidentiality of specific information. It also discusses the cyber security strategy for the Smart Grid and the specific tasks within this strategy.

Chapter 2 – Logical Architecture includes a high level diagram that depicts a composite high level view of the actors within each of the Smart Grid domains and includes an overall logical reference model of the Smart Grid, including all the major domains. The chapter also includes individual diagrams for each of the 22 logical interface categories. This architecture focuses on a short-term view (1–3 years) of the Smart Grid.

Chapter 3 – High Level Security Requirements specifies the high level security requirements for the Smart Grid for each of the 22 logical interface categories included in Chapter 2.

Chapter 4 – Cryptography and Key Management identifies technical cryptographic and key management issues across the scope of systems and devices found in the Smart Grid along with potential alternatives.

Appendix A – Crosswalk of Cyber Security Documents

Appendix B – Example Security Technologies and Procedures to Meet the High Level Security Requirements.

NISTIR 7628 - Vol 2
Guidelines for Smart Grid Cyber Security:
Vol. 2, Privacy and the Smart Grid
The Smart Grid Interoperability Panel – Cyber Security Working Group
August 2010.

Chapter 5 – Privacy and the Smart Grid includes a privacy impact assessment for the Smart Grid with a discussion of mitigating factors. The chapter also identifies potential privacy issues that may occur as new capabilities are included in the Smart Grid.

Appendix C – State Laws – Smart Grid and Electricity Delivery

Appendix D – Privacy Use Cases

Appendix E – Privacy Related Definitions

NISTIR 7628 - Vol 3
Guidelines for Smart Grid Cyber Security:
Vol. 3, Supportive Analyses and References
The Smart Grid Interoperability Panel – Cyber Security Working Group
August 2010.

Chapter 6 – Vulnerability Classes includes classes of potential vulnerabilities for the Smart Grid. Individual vulnerabilities are classified by category.

Chapter 7 – Bottom-Up Security Analysis of the Smart Grid identifies a number of specific security problems in the Smart Grid. Currently, these security problems do not have specific solutions.

Chapter 8 – Research and Development Themes for Cyber Security in the Smart Grid includes R&D themes that identify where the state of the art falls short of meeting the envisioned functional, reliability, and scalability requirements of the Smart Grid.

Chapter 9 – Overview of the Standards Review includes an overview of the process that is being used to assess standards against the high level security requirements included in this report.

Chapter 10 – Key Power System Use Cases for Security Requirements identifies key use cases that are architecturally significant with respect to security requirements for the Smart Grid.

Appendix F – Logical Architecture and Interfaces of the Smart Grid

Appendix G – Analysis Matrix of Interface Categories

Appendix H – Mappings to the High Level Security Requirements

Appendix I – Glossary and Acronyms

Appendix J – SGIP-CSWG Membership