E-RISE 2013 – Electrical Transmission Case Study

1. Introduction

This document introduces electricity transmission as the case study for assessment on the Engineering of Risks and Security Requirements (E-RISE) Challenge 2013. This case study focuses on the electricity transmission network and service that National Grid plc provides in the United Kingdom.

2. Background of National Grid

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

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

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

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

3. Electricity Transmission in the UK

To understand electricity transmission it is first useful to understand the electricity delivery or supply chain. Specifically that is how electricity is generated, transported and delivered to homes and businesses across the country. Figure 1 below shows the full lifecycle of

electricity from generation to distributor substation down to residential customer/consumer.

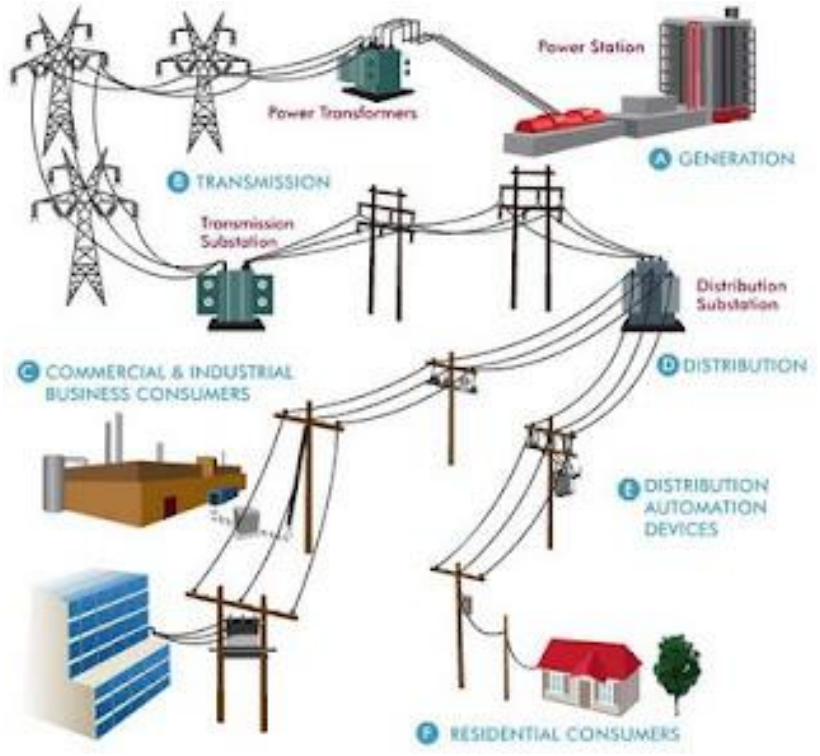

Figure 1 – Complete lifecycle of electricity delivery in the UK

At a high level the components of the electricity delivery chain are as follows:

a) Generation
b) Transmission
c) Commercial & Industrial Business Consumers
d) Distribution
e) Distribution Automation Devices
f) Residential Consumers.

Previously, when electricity delivery was a nationalised industry, one or two organisations where responsibility for generating and delivering electricity to households. The unbundling of the electricity delivery chain means that different organisations operate and manage different parts of the chain:

- There are a number of organisations that own and operate the varying generation sites,
- National Grid operates the transmission network across the UK,

- Distribution is regionalised and different companies operate the distribution network in the different regions of the UK, and
- Energy suppliers buy electricity on the wholesale market and sell it to the end customers.

National Grid, as the electricity transmission licence holder in the UK is responsible for:

- Managing the electricity transmission network and all it's associated infrastructure to ensure that electricity is delivered from the generation sites to all the regions of the country safely
- Balancing the supply and demand of electricity across the network
- Operating the wholesale electricity market.

In the next subsections we discuss these different responsibilities and bring it together in a high-level architectural diagram.

3.1 Managing the Network

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

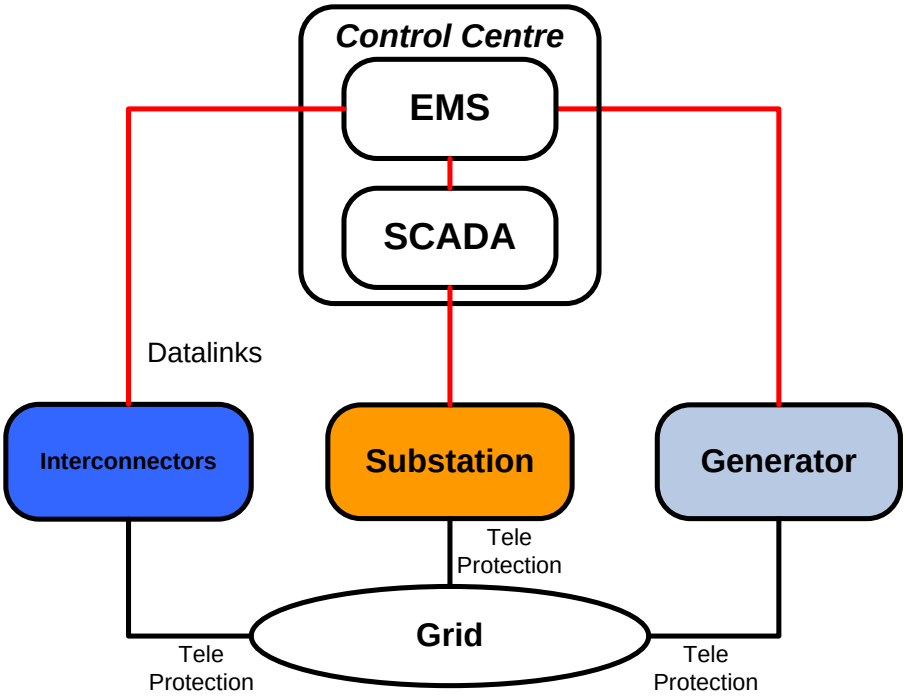

Figure 2 – Data links between the Control Centres, Interconnectors, Generators and Substations

Figure 2 shows the data links between the control centres and the interconnectors, generators and substations. The black lines between the interconnectors, generators and substations denote the actual power lines that connect these entities. Tele-protection systems are in place for safety across the high voltage power lines to stop live wires coming into to contact with commercial buildings, homes, vehicles and people.

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

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

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

3.2 Balancing the Network

National Grid are also responsible for managing the wholesale market of electricity as they understand and can forecast electricity demand across the network for future time periods. In any 30 minute time period there is an electricity demand forecast and contractual agreements with generators as to how much electricity they will provide. Prior to the actual time the market for wholesale electricity will balance this so that enough electricity is supplied given the expected demand. However, this is just a forecast and the actual demand may vary.

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

The frequency control algorithms and mechanisms decide when to increase or decrease the output of electricity at the different generation sites in order to balance the network. For

example if frequency of the system starts to fall below 50Hz this shows demand is outstripping supply. Therefore at the pre-determined trigger point the frequency system will ask for increased output from the appropriate generators, which in turn will increase the frequency back to 50Hz.

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

- National Grid need to be able to anticipate demand at time periods in the future to forecast how much electricity needs to be generated in advance
- The varying generation sites have different:
    - base loads: the amount of energy that they always produce unless the generation site is turned off
    - electricity output that can be ramped up or down
    - lead times or speed at which the site can increase or decrease electricity output
- National Grid must always have reserve output on standby for unexpected demand increases.

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

At the current time the process of balancing is not an automated. There are a variety of communication links between the control room and generators including telephone lines which operators use to speak to the generators. In the future, control of certain fast reacting generation sites may reside within the control room allowing for automated control of generation sites within agreed contractual limits.

3.3 High-Level logical diagram

Figure 3 below presents a high-level logical diagram of electricity transmission putting together the information about the SCADA and control systems as well as managing and balancing the network as described in the previous two subsections.

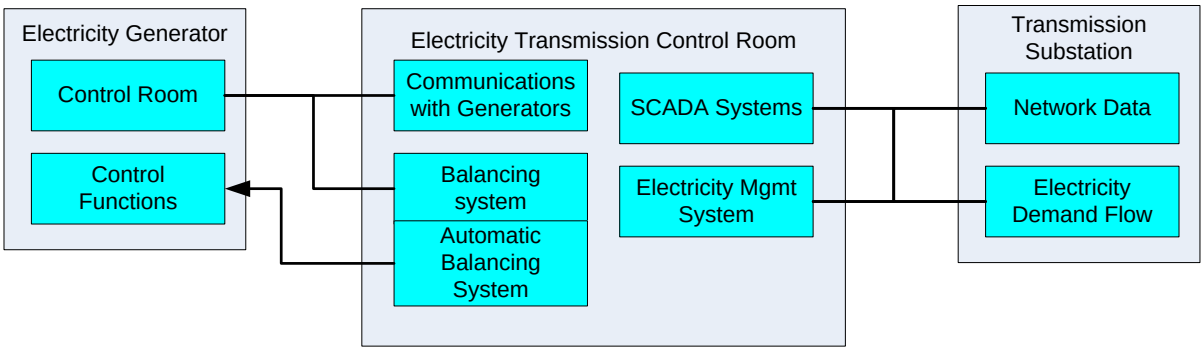

Figure 3 – High-Level Logical Diagram of Electrical Transmission

3.4 Network Data

In the managing and balancing the electricity transmission network, data needs to flow from the transmission substations and electricity generators to the transmission control rooms and vice versa.

The Transmission Substations throughout the country provide information to the SCADA systems in the control room about the network (right-hand side of Figure 3). This includes information about:

- The transmission lines operational status i.e. operational or out of service for maintenance, faults etc.
- The maximum load capacity through each line and major junction
- The current load through each transmission line at the given time
- Current electricity demand at each substation.

These substations also provide more detailed information about the actual infrastructure status including:

- The temperature of transmission lines across the network
- The temperature, air flow and other operational condition of the substation equipment.

From all of this information the control room staff are able to determine not just how much electricity needs to be generated at any specific time but also how that electricity can be routed to where it is needed in the country. Specifically, as transmission lines go in and out of service, the control room have to ensure that sufficient lines are in place to carry the load without voltage problems and lines overheating.

The information from the Transmission Substations is time critical but as time moves forward old data becomes less sensitive. Control room operational data as well as data that feed into the SCADA system is stored in multiple secure data centres around the country. These data centres are dedicated to National Grid due to their sensitivity and are run by both National Grid and contracted workers through a single vendor with a background in government systems. The data centres have dedicated fibre-optic lines to the control rooms.

The left hand side of Figure 3 presents the supply-side of electricity transmission. National Grid, through operating the market for wholesale electricity, has many contracts with the different generators that cover emergency generation, black-start scenarios, normal SLAs for day-to-day generation including ramp-up and ramp-down times as well as other situations. At any given time, there are agreements with specific generators to generate a certain amount of electricity given the forecasted demand. For each time period all generators then provide data to the control room on:

- The amount of electricity that they will generate
- The amount of capacity that they have to increase/decrease generation
- The ramp-up/down times for changes in generation.

This provides vital information to the control room about which generation sites they can call upon when demand is different from the expected forecast. When the control room calls upon a generation site to increase or decrease generation there are generally two ways in which they can do this. Primarily, applications on the IT networks within the control rooms provide electronic means to send official requests to generators. These requests are secured using various cryptographic controls to ensure integrity of the information, authenticity of the sender and non-repudiation of the sender and receiver. As a backup to this, a dedicated telephone system between all the generators and the control room is in place should the electronic dispatch system be unavailable.

3.5 Actors

The managing and balancing of the electricity transmission grid requires personnel. Both the Electricity Generators and Electricity Transmission Control Rooms have operators and managers who oversee the work of the operators.

Electricity Generator operators and managers:

- Operate and manage the output of the generation plant directly through bespoke industrial control systems
- Act upon requests from the transmission control room to increase/decrease generation.

Electricity Transmission Control Room operators and managers view and act upon information aggregated by the SCADA equipment. Broadly they use this information to:

- Manage the transmission network to ensure transmission lines are used appropriately and that there is redundancy throughout the network if a fault occurs in a line
- Balance the network by monitoring the information and communicating with the generators to ensure supply of electricity is meeting demand.

The Transmission Data Centres are managed by experienced IT technicians that ensure that the systems are running smoothly. For resiliency multiple servers and systems are in place to support the SCADA and Electricity Management System. Therefore faults do not interrupt the system's service levels. The IT technicians manage the effective and efficient running of the servers and systems, part of which is to fix faults in a timely manner to keep the resiliency of the system as a whole.

The Transmission substations are generally unmanned as there are many of them across the country. Remote Telemetry Units (RTUs) within the substations provide the network data that feeds into the SCADA system. Engineers have access to substations if there is a need to perform maintenance, repair or renovation or simply to monitor the equipment if an RTU fails.

4. Previous Blackout Incidents

In recent years there have been a number of incidents to electricity transmission grids across the world resulting in power outages to large numbers of people for significant

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

A sample of these incidents has been described below:

- In September 2003 there was a major blackout in Italy cutting service to a total of 56 million people. Italy was mainly affected as well as parts of Switzerland, Austria, Slovenia and Croatia. The blackout was the result of a power line between Switzerland and Italy being damaged causing a cascade effect resulting in generation sites to trip. Consequences of the outage were failures in the public transport sector, the publishing of newspapers and mobile phone links. The health sector continued operating using reserve power generators and the overall initial impact was less dramatic as it happened on a weekend night.
- On 14 August 2003 there was a major blackout in the USA and Canada affecting over 45 million Americans and 10 million Canadians. It was caused by a high-voltage power line which brushed against some overgrown trees in Northern Ohio that resulted in a shut down causing other generation sites to follow. The system which would normally have tripped an alarm in the control room failed. The heat of August triggered the outage, because the energy demand increased as many people turned on fans and air conditioning. The result was a wide-area power failure in the North-eastern USA and central Canada. The affects on the general public was a loss of power for up to two days. Some cities water systems lost pressure, the telephone circuits were overloaded, the cellular service was interrupted, but most television and radio stations remained on the air, because of the help of backup generators. Most of the public transport system and financial markets were interrupted and affected.
- On the 30 July 2012 there was a significant electricity outage in the North of India, which is one of the biggest power failures in the world to date. It was caused by record power demand due to extreme heat. In the Punjab and Haryana states, the agricultural industry used power from the grid for running irrigation pumps as the monsoon session had arrived late. Due to the increased power use, the 400 kV Bina-Gwalior line tripped, which led to the tripping of power stations. The outage affected seven north Indian states and more than 300 million people were without power. Traffic signals were non-operational, some airports and railways were shut down, and this resulted in major transport problems during the Monday morning rush hour. Additionally the health sector was affected as several hospitals, without backup generators, had their health services interrupted. Water treatment plants were also shut down for several hours, leaving millions without water and businesses were impacted due to leaving many unable to operate. After 15 hours 80% of service was restored. However, the following day, the previous affected regions were again without electricity and at the same time the eastern Indian grid failed as well, with the North-Eastern grid tripping out shortly afterwards. The factors leading to the outages were the weak inter-regional corridors due to the multiple outages the day before, the high loading on the Bina-Gwalior-Agra link and the tripping of this link as a result. Most of the 48,000MW demand load was affected but a few regions of the

country continued to have power. Half of India was left without an electricity supply and over 620 million people were affected. The electricity was restored in the affected regions between 31 July and 1 August 2012 but the impact on the society was significant, as some hundred thousand people were stuck in the public transport system, airports were using generator backups and 200 miners were trapped underground.

5. Previous Malware Incidents affecting SCADA systems and Electricity Transmission Networks

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

In recent years there have been information/cyber security incidents on SCADA systems, electricity transmission networks and their operators who are referred to as Transmission Service Operators (TSOs). These all have relevance to National Grid and the CNI it owns and operates.

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

A sample of these incidents has been described below:

- Between June 2009 and the beginning of 2011 there was a major malware attack on Iran's uranium enrichment program. Before the malware, named Stuxnet, could be finalised and attack the program there had been a prior stage. A cyber espionage tool was used as a precursor to Stuxnet in order to gain information about technical configurations and operations in the plant in Natanz to design the Stuxnet code. Stuxnet was designed to attack the centrifuges used to enrich uranium and, to ensure the attack was not mitigated, also attacked the SCADA systems which provided operational control for the infrastructure and production networks. Its specific purpose was to corrupt the Siemens' Simatic Wincc SCADA system. Stuxnet intercepted commands sent from the SCADA system to control a certain function at the plant. The malware replaced the intercepted commands with malicious commands in order to manipulate the system. This resulted in the malfunction of the SCADA system without anyone recognising the impact on the uranium enrichment. After some changes on the system by the attackers, the worm spread wider than intended. Stuxnet-like malware are highly dangerous, because they are capable not only of affecting computer systems across a network, but they are also able to cause physical damage to the equipment that these computer systems control.

- In 2010, a year after Stuxnet was discovered, another piece of malware using some of the same techniques was found. This malware, named Duqu, infected systems in Europe and it has been presumed that it was written by the same authors behind Stuxnet. Like Stuxnet, Duqu masks itself as legitimate code as a driver file with a valid digital certificate. The difference is that this malware is not a worm as it does not self-replicate in order to spread. It is thought to have been a precursor to a Stuxnet-like attack. Its purpose was to conduct reconnaissance on an unknown industrial control system and gather intelligence for a possible targeted attack later. Whilst not having the components to attack SCADA systems directly, it is still a danger for SCADA systems due to its similarities to Stuxnet.
- In May 2010 the malware Flame, also known as sKyWIper, was created as a cyber espionage tool. Compared to Duqu it is significantly more complex. Flame is an attack toolkit and has worm-like features. These features allow Flame to replicate in a local network and on removable media. Once Flame has infected a system, it begins a complex set of operations, including sniffing the network traffic, taking screenshots, recording audio conversations, intercepting and recording keystrokes on keyboards and so on. The data is then available to the operators and the operators can even expand the functionality after the malware has been deployed. The purposes of the malware are still being investigated, because it contains about 20 modules in total.
- More recently, in November 2012 the German 50 Hertz grid company was the subject of a botnet attack from Eastern Europe. 50 Hertz's web servers were blocked after the attack by the hackers using a Distributed Denial-of-Service-Attack (DDOS). It is believed that the attackers did not aim to disturb the control of the power grid as the computers related to the grid control do not have internet access. The attack resulted in the blockage of their intranet and internet as well as the failure of the e-mail communication internally and externally. The 50 Hertz administrators reacted by disconnecting the computers from the network and closing their website temporarily.