# Addendum to Marsh Report

# TRANSGRID - QUANTIFICATION OF SELF-INSURANCE COSTS AND ESTIMATION OF INSURANCE PREMIUMS 2014/2015 TO 2018/2019

Addendum in response to AER Draft Decision dated November 2014

**Cyber-Related External Attack**

"Beyond the control of a reasonable operator" – broadly relating to cyber threats against Utility companies:

- Utility companies (which is a broad term, but would include transmission lines operators) are attractive to **cyber terrorism** by their very nature
  - Cyber terrorists want to cause mass disruption and/or loss of life
  - Raids on Al Qaeda bases in Pakistan uncovered stockpiles of information on SCADA systems according to news reports in 2010
  - In Aug 2010 a computer worm which disrupted corporate computer systems in the US was linked to a Libyan hacker suspected of trying to form a hacking group

- Utility companies (again including transmission lines operators) are also a target for **Hacktivist groups**
  - Environmentalists in the past have targeted power stations with physical disruption, it follows that cyber disruption may follow
  - In August 2012 a group in Canada "Integrated Terrorism Assessment Centre" issued a memo warning stakeholders in Alberta's Oil Sands that groups motivated by environmentalism were targeting the company
  - In 2010 hacktivists hijacked the web page for the EU's cap and trade scheme, replacing it with a website detailing the scheme's shortcomings

Specific to an attack on the SCADA System:

- SCADA systems purported to be separate from the internet often turn out to be connected in some way
  - Rudimentary hacking techniques such as port scanning and password guessing are usually all it takes to hack into a SCADA system once a connection is made.
  - In cases when monitoring a process geographically removed from the monitoring station, Virtual Private Networks (VPNs) are used to link systems – with an internet connection in place, there are thousands of ways to gain access

- Two types of Cyber Attacks against SCADA Systems have been identified:
  - Targeted Attacks which are written to damage or control a particular system in a specific organisation – Stuxnet[1]** is an example of this type of attack
  - Opportunistic attacks which carpet bomb targets in the hope that some will have the vulnerabilities necessary for infection

[1] Stuxnet –This occurred in Iran in July 2010. Stuxnet is believed to have changed temperature parameters minutely, so as not to raise any alarms whilst still disrupting the development of uranium. This is an example of how once a virus or computer worm accesses the SCADA system, there are various ways it might work – including data acquisition, asset deletion and disruption. The form disruption takes depends upon the type of physical entity the SCADA system controls. In cases where the system is highly sensitive, causing a process to operate just slightly outside of its usual parameters may be enough (and yet disguising the disruption from view)

- Potential Entry systems for a hack into SCADA include Internet connections (as per above); local networks which may contain wireless elements which can be used as back door entry points for malicious intruders; physical access – regardless of the most advanced security systems available, an unattended work station or determined insider could still cause disruption

In other cases, programmable switches were simply turned on and off repeatedly in order to break or damage hardware.

Following are some other examples for consideration:

**NEW MEXICO WIND TURBINE**

| | |
|---|---|
| **When** | 14 April 2011 |
| **Who** | An intruder using the alias 'Bgr R'<br>A 'disgruntled' former employee of Florida Power & Light Co (a sister company) claimed to hack into the company |
| **Where** | Fort Sumner wind turbine facility, owned and operated by NextEra Energy Resources, the primary provider of wind and solar power in North America |
| **What they did/stole** | They posted an entry to the full disclosure mailing list claiming to have successfully broken into Fort Sumner<br>The hacker supposedly exploited a vulnerability in the company's Cisco security management software to gain access into the SCADA system<br>The hacker included apparent screen shots of the facility's wind turbine management interface, an FTP server and a project management system |
| **How** | Some argue whether the hack was legitimate or whether the former employee abused legitimate access rights to penetrate the SCADA system |

MARSH

## STUXNET – Advanced Infection Strategies

| | |
|---|---|
| **What they did/stole** | Stuxnet utilised a variety of tactics to gain access to its intended target<br>The virus was targeted at unsecured computers whose owners were affiliated with Iran's nuclear programme. It was programmed to automatically replicate itself onto any removable drive they connected in the hope that these drives would later be plugged into the target systems |
| **Why** | Political at first |
| **How** | These targets were not connected to the internet and were not part of a broader network<br>In order to access them Stuxnet exploited a Windows vulnerability allowing for auto-execution of files on a removable drive<br>Other techniques for helping the virus spread include an exploitation of the windows printer spooler and targeting of shared drives<br>Insider help cannot be ruled out |

## PUBLIC WATER SYSTEM IN SPRINGFIELD ILLINOIS, USA

| | |
|---|---|
| **When** | Discovered on 8 November 2011 (believed to be there 2/3 months before they were discovered) |
| **Who** | Hackers traced back to Russia |
| **Where** | Public water system in Springfield, Illinois |
| **What they did/stole** | Accessed the water plant's SCADA online control system<br>Stole customer usernames and passwords, in order to gain remote access to the utility's network<br>A water pump was then repeatedly turned on and off causing it to burn out |
| **How** | FBI questioning if this was really a hack or employee negligence |

## OTHER ATTACKS

- The Central Intelligence Agency has issued alerts about the threat of cyber warfare, including forays by agents in China and Russia that penetrated and thus 'owned' American utility networks. Many of these intrusions were detected not by utility companies but by the intelligence agencies
- In 2007, the U.S. Department of Energy researchers in partnership with the U.S. Department of Homeland Security launched an experimental, yet realistic, cyber-attack dubbed 'Aurora.' The simulated attack caused a generator to self-destruct by exploiting vulnerabilities found in the grid
- A recent survey of utility executives by Logic reported that half of all utilities experience more than 150 attacks per week

**In summary, given the sophistication of a Stuxnet type of disruption, we believe that an attack on a SCADA system is definitely beyond the control of a reasonable operator.**