



<http://d2.cigre.org>  
/

CONSEIL INTERNATIONAL DES GRANDS RESEAUX ELECTRIQUES  
INTERNATIONAL COUNCIL ON LARGE ELECTRIC SYSTEMS

**STUDY COMMITTEE D2**  
INFORMATION SYSTEMS AND TELECOMMUNICATION

**2017 Colloquium**  
**September 20 to 22, 2017**  
**Moscow – RUSSIA**

**Preferential Subject N° - PS2: Resilience to cyber threats of information and telecommunication systems in the power industry**

**Cyber-threats and the Risks They Pose to Power Utilities**

**B PETZER**  
**Eskom**  
**South Africa**  
**PetzerB@eskom.co.za**

Cyber threats to the energy sector are becoming a growing concern worldwide. Cyber-attacks, such as those recently mounted on Ukraine power companies, have led to large power outages that lasted for several hours. These occurrences serve to emphasise how vulnerable energy utilities currently are in the connected world, and increasingly becoming so.

With the progression to smarter grids, the growing popularity of Independent Power Producers and the rapid growth of The Internet of Things, our operational technology environments are no longer as isolated as they used to be, but are becoming connected to corporate networks and the Internet through necessity. Our internal telecommunications networks can now be used against us. For business intelligence and specific engineering applications (e.g. distributed management systems, engineering servers, and substation watchdogs), it is becoming unavoidable that data flow between corporate networks and industrial environments. It is therefore of paramount importance to adequately protect ourselves, as attacks on the grid might not only cause discomfort or financial loss, but lead to more severe repercussions such as crippling whole economies or even loss of human life.

This paper will therefore cover:

- Growing cyber security trends worldwide, with a focus on the power industry
- Threats specific to power utilities
- Most common cyber-vulnerabilities of power utilities
- Measures for utilities to protect against cyber attacks

A look will be taken at some security principles that need to be taken into consideration in the operational technology environment of power utilities (including telecommunications infrastructure and substations), secure network design, and measures we need to have in place to mitigate risks and aid in responding to and recovering from cyber-attacks. The role of

	<p style="text-align: center;">CONSEIL INTERNATIONAL DES GRANDS RESEAUX ELECTRIQUES INTERNATIONAL COUNCIL ON LARGE ELECTRIC SYSTEMS</p> <p><b>STUDY COMMITTEE D2</b> INFORMATION SYSTEMS AND TELECOMMUNICATION</p>
	<p style="text-align: center;"><b>2017 Colloquium</b> <b>September 20 to 22, 2017</b> <b>Moscow – RUSSIA</b></p>

<http://d2.cigre.org>

/

regular employees and the cyber-risks that they inadvertently pose to power utilities will also be discussed.

The aim of this paper will be to create awareness, educate and also galvanise those who work in the power industry. It is important that power companies across the world learn from one another, discuss challenges and work collaboratively to create both awareness and achieve security to better protect their grids.