NAME : Doug Ray (presenter)	GROUP REF. : SC B4
COUNTRY : New Zealand	PREF. SUBJECT : 1
REGISTRATION NUMBER : 7366	QUESTION N° : 5

How should the existing HVDC installations manage the security issues and updates? How can the lifetime of control systems be extended?

Transpower's experience with HVDC Life Extensions

Where Windows based operating systems are used on HVDC installations, one key challenge that the owners may experience is operating with outdated Windows operating systems. This may expose the system to security vulnerabilities as well as hardware issues. In some cases, upgrading of the operating systems may not be possible due to limitations with vendor specific applications.

In the case of having to operate computers with obsolete operating systems, virtualisation of these computers inside more secure operating systems running on modern hardware can be a good temporary solution. This would minimise the security risk while also addressing any hardware issues. In some cases, outage requirements will restrict implementation of a longer-term solution, necessitating the use of temporary interventions such as this.

Extensive investigations into operational threats and addressing of identified vulnerabilities is also important. Taking all reasonable steps to minimise the impact of a breach is also important as already discussed in many CIGRE documents. This may include preparations such as taking regular images of the computers. Having in-house expertise would be valuable in managing technical risks and in the case of restoring the system following a cyber-attack.

Once the owners get notices from the vendors around life cycle activities such as phasing out of any control cards, consideration could be given to purchasing additional spares while hardware is still available. This will minimise the risk of obsolescence.

Geethma Dissanayake / Michael Dalzell, Transpower, New Zealand