Author
Roger Pan is the security program manager for Emerson Process Management's Power & Water Solutions. For the last 10 years, he has focused on control system cyber security. With an in-depth knowledge of security processes and procedures, he has significant experience developing and deploying security products for control systems, conducting onsite security assessments for utilities and other related activities.

KEEPING SECURITY UNDER CONTROL Roger Pan, Emerson Process Management, US

If you've worked in the power industry for the last 20 years or so, you can most likely remember when security by obscurity was largely deemed to be sufficient for plant automation and control systems. These control systems were originally built using proprietary software protocols, which served as a kind of invisibility cloak that shielded them from the outside world. That way of thinking became obsolete as power plants turned away from proprietary systems and toward controls based on open standards.

Moving to commercial, off-the-shelf, technologies offered numerous benefits to utilities: e.g., the ability to cost-effectively take advantage of the latest advancements in computing. On the other hand, it also put an end to security by obscurity and created a need for organisations to be more vigilant in actively assessing potential vulnerabilities and adopting cyber-security measures.

In recent years, there has been a growing urgency surrounding cyber security. This is evident from scanning the content of media outlets from around the world: from V3.co.uk to *The Journal of Turkish Weekly*, the need to keep critical infrastructure secure is headline news.

Government reports are another source of this urgency. Late last year, the US Department of Homeland Security (DHS) reported an increase in cyber attacks aimed at energy and pipeline infrastructure worldwide. The statistics are sobering: 40% of the 198 incidents reviewed by the DHS Industrial Control Systems (ICS) Cyber Emergency Response Team (CERT) in 2012 were associated with energy businesses.

Some cyber security breaches are caused by sophisticated hackers. Others have been caused by something as seemingly harmless as a USB drive. According to a recent issue of the ICS-CERT newsletter, two US power plants had been infected with computer viruses through USB drives. One of the incidents involved an infected turbine control system. The virus, which spread during a scheduled outage for equipment upgrades, delayed plant restart by roughly three weeks. While this was costly in terms of time and lost MW, the price could have been much higher had the virus not been detected.

In the US, the North American Electric Reliability Corp.'s (NERC) Critical Infrastructure Protection (CIP) standards continue to evolve. NERC, an organisation focused on improving the reliability and security of the bulk power system in North America, created CIP standards that detail the action power generation companies must take in order to protect their critical assets. Generally speaking, these assets include computers, software and SCADA and process control systems related to the reliable operation of bulk electric systems, as well as the networks that support them.

NERC CIP Version 4, approved by the Federal Energy Regulatory Commission (FERC) in April 2012, was to become effective on 1 April 2014. However, in April 2013, FERC issued a notice of proposed rulemaking (NOPR) in which it proposed to approve NERC CIP Version 5 and to transition directly from CIP Version 3 to CIP Version 5, bypassing the implementation of the CIP Version 4. An executive order on critical infrastructure cyber security signed by President Barack Obama in February is believed by some to be the driving force behind the rapid movement.

> WHEN IT COMES TO CYBER SECURITY, CHANGE IS THE ONLY CONSTANT.

Keeping up-to-date on changes to the CIP standards and preparing for compliance can be difficult for utilities, particularly when considering the many demands placed on plant personnel. Fortunately, they have an ally in reputable automation and control system suppliers.

The security capabilities of control systems are not all created equal. For that reason, every utility needs to assess the capabilities of its control system supplier specifically as it relates to cyber security. One way to start tackling this is by developing a checklist that addresses key areas of concern. While one of the sample questions below pertains specifically to NERC CIP, the majority of questions would apply to power generators in all parts of the world, as cyber security is a concern that knows no borders.

- Does the supplier speak the language of cyber security?
- How often does the supplier communicate about the security features of their system?
- Does the supplier proactively communicate about how security features are updated to address new and/or changing security threats?
- Is the supplier aware of the latest developments in NERC-CIP standards and how they might impact generating assets?
- Does the supplier have the expertise necessary to help assess vulnerabilities at plants?
- Does the supplier understand the implications of cyber security for the entire organisation – from the plant level to the corporate IT level?

When it comes to cyber security, change is the only constant. New viruses and other, increasingly sophisticated, cyber threats require constant vigilance. Independent of the pending NERC standards and other security efforts in the industry, it is important to remember that control system security has always been a top priority for reputable control system suppliers and their customers. To keep ahead of changing security issues and potential threats, proactive suppliers provide enhanced security features, functions and services to their systems on a continual basis. They also work with customers to test and validate new tools and features to ensure they meet real-world security needs.

A control system supplier should also understand that security is just one of many demands the industry faces. The supplier should, therefore, offer solutions that make complex security issues easy to manage as part of an overall automation and control system strategy. These solutions should be able to be tailored to a power generator's specific needs at the corporate, fleet, plant or unit level and be adaptable to address evolving security concerns. Doing so will help ensure the efficient, reliable and secure operation of power plants today and well into the future.