



# *Better safe than sorry*

**Protecting critical power generation assets is vital to ensure worker safety and avoid loss of revenue and increased wear and tear on plant equipment, says Mark Boyes**

Without a current international or European standard on cyber security, many European utility companies are adopting the Critical Infrastructure Protection (CIP) standards developed by the North America Electric Reliability Corporation (NERC), an organisation focused on improving the reliability and security of the bulk power system in North America. This standard was written in the wake of the terrorist attacks of September 11 2001 and in response to a challenge set by the US government to protect power generation assets against the threat of attack.

The CIP standards detail the action that power generation companies must take to protect their critical assets such as computers, software, supervisory control and data acquisition (Scada) and process control systems, and the networks that support those systems.

Each of the eight discrete NERC CIP standards tackles a different aspect of IT security, such as personnel and training, incident reporting and response planning, and recovery plans. Distributed control systems (DCSs) are the focus of Standard CIP-007-01: Systems Security Management, which addresses 11 requirements including test procedures for both attended and unattended facilities, account and password management, security patch management and integrity software.

NERC has set out a phased, yet aggressive, timetable for compliance, which concludes on

31 December 2010, when plant owners and operators must be compliant and have the records to prove it.

Although the exact details of CIP standards continue to be refined, they are a valuable guide to securing critical cyber assets that can be adapted by energy companies in Europe.

The need for vigilance – even in the absence of government-imposed mandates – is compelling. Not so long ago, energy companies relied primarily on security by obscurity to thwart potential attacks on their power generating facilities. By and large this was sufficient, as the use of proprietary software and protocols protected DCSs from the outside world.

But times have changed. As the world's energy needs grow, power generators are responding by constructing new plants as well as applying automation, instrumentation and equipment upgrades designed to extend the life of older plants. These new and modernised facilities are equipped with sophisticated, state-of-the-art DCSs that rely on open standards such as ethernet, TCP/IP and web technologies, as well as commercial off-the-shelf (Cots) hardware and software. Open standards and technologies offer significant advantages, including the ability to adopt and maintain the latest and best technologies more easily, quickly and cost-effectively. Clearly, there is no turning back the clock and returning to the era of proprietary systems.

Adoption of open standards and Cots does, however, require organisations to be more vigilant in proactively assessing potential vulnerabilities and adopting cyber security measures.

External attacks, in the form of viruses, worms and other products of malicious hackers, are an increasing concern. The Davis-Besse nuclear power plant in the US state of Ohio was infected with the MS SQL Server 2000 "slammer" worm in January 2003 by a trusted third-party connection. The infection caused data overload in the site network, and its computers lost the ability to communicate with each other. This attack, though relatively minor in scope and damages, illustrates the potential for malicious cyber activity in the control networks and systems of the electric power industry.

While hackers intend to cause disruption, it is also possible for potentially serious cyber security breaches to arise from sources that are neither hostile nor malicious. For example, *The Japan Times* reported that security data on a thermal power plant owned by Chubu Electric Power was leaked onto the internet from a virus-infected personal computer belonging to an employee of the plant's security firm. Data that unwittingly found its way onto the internet included information about the plant's control room, instrument panel room and boilers, as well as security manuals and other information about the plant's security personnel.

For the greatest effect, initiatives to improve DCS security should be part of an enterprise-wide risk management programme – not merely adopted on an individual plant basis.

The reasons are convincing. The consequences of an unplanned unit shutdown can include significant lost revenue, high plant restart costs, and increased wear and tear on plant equipment. Improper operation can also lead to very costly equipment damage and even multi-million pound damage in the event of turbine rotor failure. Improper operation or shutdown as a result of a cyber attack can jeopardise worker safety, while an attack during peak load periods can cost the power generation company in the order of £2 million per incident in lost revenue.

Also consider that many power plant owners/operators have implemented measures to improve plant efficiency without necessarily considering the effect of their actions on plant security. In addition to standardising technologies (Cots, etc) used in DCSs, other activities that can compromise security include expanding DCS access to company personnel on the company network (financial analysts, market traders and engineering operational staff) and enabling users to access the control system remotely in an effort to improve fuel economy, maximise plant output, reduce maintenance costs and increase profit.

The two groups that must jointly address plant security – IT personnel and plant operations personnel – traditionally do not work closely

together. Although IT departments understand the need for improved systems security, they may not have direct control over practices adopted in the power plant. These are usually the responsibility of plant managers, who are primarily interested in uninterrupted, safe operations and may not fully comprehend the need for improved DCS security.

In an attempt to address this, many IT managers at power generation companies in the US are now creating "action groups" with the most proactive plant managers to address security measures and then propagate them across the company.

Rather than waiting for electronic security vulnerabilities to be exploited, power generators need to anticipate and analyse possible avenues of attack. There are a variety of tools available to help assure DCS security:

- Hardening, which disables unused ports and services. Because cyber attacks target ports and services, removing those that are not used (email, for example) lowers the system's profile, making it less vulnerable to attack;
- Anti-virus software, which protects the system from malicious programs spread by unsuspecting users;
- Intrusion detection systems (IDSs), which protect the system from hackers and worms, which are viruses that reside in the active memory of a computer and duplicate themselves, potentially wreaking havoc.

Of course, technology is just part of the security equation. Cyber security measures are most effective when they also identify and address the human factors that can lead to security breaches. While the first reaction may be to view cyber security from a perspective of protecting operations and processes from intentional, malicious intrusion, a security breach may in fact be set in motion by an employee who has let down their guard.

The best way to address the human side of the equation is training and education. The focus here is to not only ensure employees know the policies and procedures, but that they also think about their actions and understand the ramifications.

To date, the US has taken the lead in developing standards pertaining to cyber security of the country's power generating facilities. However, it is incumbent upon energy producers in countries that have yet to impose regulations to proactively implement cyber security measures for their fleet of generating assets. Choosing not to act until directed to do so is risky at best. Given the tremendous and potentially detrimental consequences of inaction, when it comes to protecting critical cyber assets, "better safe than sorry" is an adage worth heeding. ●

*Mark Boyes is director, project and service operations UK, at Emerson Process Management ([www.emersonprocess.com](http://www.emersonprocess.com))*

**An attack during peak load periods can cost the power generation company in the order of £2 million per incident in lost revenue**