WHITE PAPER: ENTERPRISE SOLUTIONS

Effective Practices for Securing Distributed Control Systems in Power Generation Facilities

White Paper: Symantec Enterprise Solutions

Effective Practices for Securing Distributed Control Systems in Power Generation Facilities

Contents

Executive summary

The North American Electric Reliability Council (NERC) Critical Infrastructure Protection (CIP) standards, which will take effect in November 2005, require power generation companies to protect their assets from cyber security attack. Yet securing the Distributed Control Systems (DCSs) that control most U.S. and worldwide power plants is becoming an increasingly complex task. To compete in the deregulated market of power generation, power plant owner/operators have implemented measures to improve plant efficiency, while maintaining plant safety. These measures have included opening DCS access to company personnel on the corporate network (e.g., financial analysts, market traders, and engineering operational staff), DCS suppliers, maintenance contractors, and others – all in an effort to improve fuel economy, maximize plant output, reduce maintenance costs, and improve the bottom line. Yet, this expanded access to the DCS provides a broader range of potential access points for malicious attackers to exploit. Standardization of DCS technologies and protocols and the need for ease of information availability on these systems is making the attacker's job even easier.

A cyber attack that shuts down a generating unit (e.g., via misinformation provided to the operator) can result in major economic costs to the unit's owner/operator and can pose worker safety risks as well. Hence, even in the absence of NERC standards, improving DCS security should be part of an enterprise-wide risk management program for power generation companies. But the challenges of securing DCSs are daunting. Security has not been the primary driver of DCS design. Moreover, the two groups in a power generation company that must jointly solve this problem – corporate IT personnel and plant operators – traditionally do not work closely together. At the same time, a general lack of awareness that the problem is serious slows progress.

This paper takes a step towards improving this awareness by describing effective practices that power generation companies can adopt to improve DCS security. Developed via a collaboration between Symantec™ and a leading power plant DCS vendor, these recommendations are organized according to a four-step cyber security process –assessment, policy, measure deployment, and monitoring/management. While these measures map closely to the NERC CIP standards, perhaps more importantly, they also make good business sense for power generation companies.

Business drivers of cyber security

Changes resulting from electric power industry restructuring have increased the need for heightened information security in this industry. In many states, unbundling of the power generation function from the power delivery and retail functions, as well as deregulation of the

power generation market, have motivated power plant owner/operators to reduce costs and improve plant operating efficiency. To do this, these owner/operators have implemented several changes and new practices that can potentially affect the cyber security of their power plants. The most significant impacts of these changes relate to the Distributed Control Systems (DCS) that are used to operate most power plants in the U.S. and worldwide today.

For example, many power plant owner/operators have added connections between their corporate computer networks and these DCSs. This interconnectivity allows corporate decision makers to obtain instant access, for example, to critical data about the status of their operating assets. During periods of peak power consumption, power plant capacity and emissions control equipment are pushed to their limits in an effort to maximize revenue at a time when deregulated power market pricing is very high. Monitoring this information in real-time aids power sales decision making and other considerations. However, this interconnection also opens new vulnerabilities to the DCS, as the corporate network then becomes a potential additional access point to the control system.

Other practices to improve plant efficiency include enabling remote access to plant DCSs by company engineers, contractors, and others via dial-in modems and other means. This allows off-site personnel to troubleshoot problems that arise in real-time from any location, thus reducing the duration of suboptimal operation. But, like the interconnection with the corporate network, this practice introduces new access points to the DCS. Figure 1 illustrates a typical DCS in relation to a corporate network.

Visiting employees from other locations, hired contractors, and other authorized parties also need to access the corporate network from their laptop computers to gather information to aid decision making and maintenance activities. Such access may, in turn, unleash viruses or malicious code on the DCS.

The drive to improve plant operation is also leading to increasing standardization of DCS technologies. DCSs are increasingly implemented on Microsoft Windows and Linux operating system-based platforms, enabling a broad range of third parties to offer software that can help optimize plant operation and maintenance techniques. Similarly, most DCSs comply with OPC (a Microsoft-based standard for open connectivity) and the protocols of major manufacturers of programmable logic controllers (PLCs) and remote terminal units (RTUs).

In parallel with this standardization trend, technical information about these standards and the DCSs themselves is becoming increasingly available in trade journals, from online information brokers, and from government agencies. This combination of standardization and widely available information enables would-be attackers to learn how a very large number of DCSs function by learning about a very small number of systems and protocols.

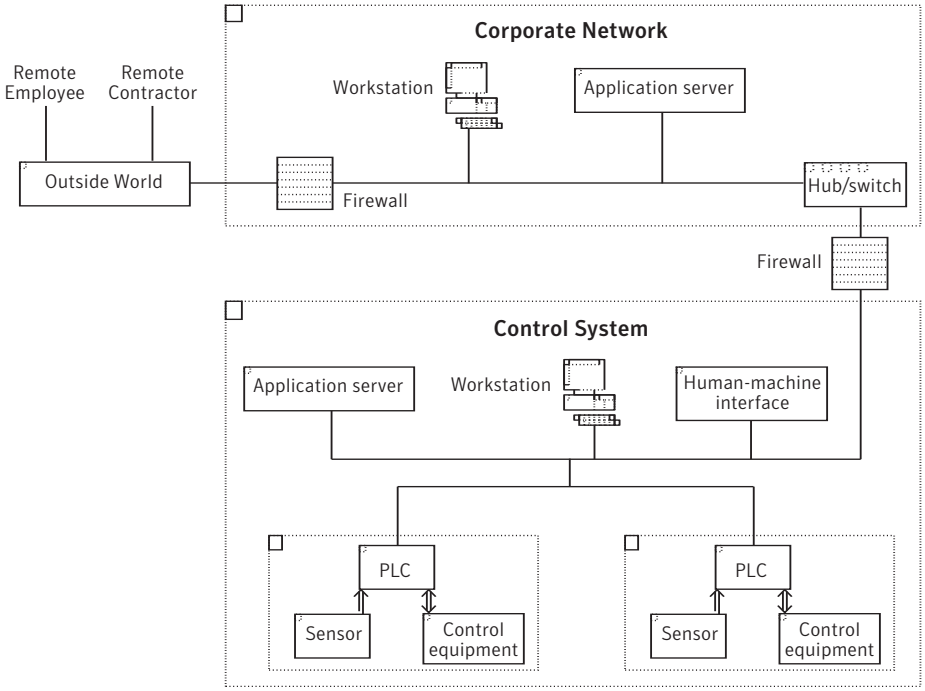

Figure 1
Typical Power Plant DCS connected to a corporate network

A recent regulatory development that heightens the urgency for cyber security measures in power plants is the North American Electric Reliability Council (NERC) Critical Infrastructure Protection (CIP) standards. An outgrowth of the temporary NERC Urgent Action Standard 1200 established in 2003 and originally named the NERC Cyber Security Standard 1300 in 2004, NERC CIP is the first set of comprehensive requirements to protect electric utility assets from cyber security attack. Its proposed effective date is November 1, 2005, and power plants will have 12 months from a "registration" date to be substantially compliant. NERC CIP establishes standards in eight key areas that are designed to protect not only power plants but all other aspects of electric utility operations and assets as well. Of particular interest to power generation owner/operators, the standard includes provisions for identifying critical cyber assets (section 002), developing security policy and governance (section 003), identifying and implementing perimeter security (section 005), protecting assets and information within the perimeter (section 007), conducting incident reporting and response planning (section 008), and crafting and implementing recovery plans (section 009).

In a second key regulatory development, the Sarbanes-Oxley Act of 2002 (SOX) was enacted in the wake of various accounting scandals. SOX requires many companies to certify the effectiveness of their information technology and financial controls when they file certain financial reports. This means that compliance with this act involves the need for accurate information. Yet, without proper security practices, company officials are unable to confidently sign off on these reports or controls. SOX also requires public disclosure in the event of revenue flow disruption as a result of a cyber incident. Because such disclosure could reduce customer confidence (and investor confidence, in the case of investor-owned utilities), reducing security risks is a high priority.

Critical nature of power plant DCSs: efficiency and safety

Since the 1980s, DCSs have played a central role in efficient and safe power plant operation – providing control during normal operations, startups, planned shutdowns, and trips, as well as providing alarms to operators, and monitoring equipment condition for maintenance purposes. The vast majority of today's power plants – including fossil fuel-fired units, hydroelectric units, and nuclear units in baseload, cycling, and peaking operation – use DCSs. Some older plants still use analog/pneumatic controls, but this is becoming increasingly rare; the demands of the new competitive marketplace make operating a unit in this manner impractical. This means that there are literally thousands of DCSs operating at power plants in the U.S. alone.

And each of these DCSs must maintain the delicate balance of optimal fuel economy (efficiency), minimized plant equipment wear and tear, maximum plant output, and maximum worker safety. By gaining cyber access to a DCS at a power plant, attackers could:

- Disrupt this balance of operating parameters, leading to a plant trip (shutdown)
- Disrupt operation in a manner that not only leads to temporary plant shutdown, but also causes permanent equipment damage
- Cause a trip and interfere with safe, proper shutdown procedures, potentially causing catastrophic damage and endangering plant personnel

Improving the security of the DCS against attacks like these involves more than simply complying with NERC CIP regulations. Attacks like these can have serious business costs and adversely impact plant worker safety. For example, the consequences of an unplanned unit shutdown can include high costs in lost revenue, high plant restart costs, and increased wear and tear on units. Improper operation can also lead to very costly equipment damage, and even multi-million dollar damage in the event of turbine rotor failure. Improper normal operation or

shutdown as a result of a cyber attack can also jeopardize worker safety (e.g., as a result of a bursting steam line that is subjected to excessive pressure). The consequences of an attack that occurs during peak load periods can include costs to the power generation company on the order of a million dollars per incident in lost revenue, and degraded wide area reliability due to loss of the generation unit. During a period of time in the electric power industry when the power grid is operating close to the limits of its capacity (due to insufficient additions and upgrades to the power delivery system), loss of even a single generating unit can be problematic.

Challenges to increasing DCS security

Cyber security was not the primary consideration when power plant DCS networks and systems were developed and installed years ago. Rather, the primary driver was the high level of plant efficiency and reliability needed. This fact is one of the challenges the power generation industry faces today when seeking to better secure DCSs. Another challenge is the interconnected nature of corporate networks and control networks, potentially enabling an attacker to access the DCS through the corporate network.

A further challenge involves the division of responsibility for enhanced DCS security between two separate groups – corporate IT personnel and control system personnel. These two groups are often disconnected from each other. While CIOs and their departments understand the need for improved DCS security, they may have no direct control over practices adopted in the power plant. This situation complicates establishment of a centralized security approach and policy at the power generation company. In an attempt to address this, many CIOs at power generation companies are creating “action groups” with the most proactive plant managers to address security measures and then propagate them across the company – one plant at a time.

A CIO and IS director of a power generation company may have scores or even hundreds of power plants in their purview, which run on different generations of DCSs from different vendors. And some power plants use DCSs from multiple vendors (e.g., one DCS vendor’s system controls the boiler, another controls the turbine, and a third controls the switchyard equipment). At the same time, lack of awareness among both plant IT personnel and engineers/operating personnel in the following areas is a concern:

- The likely existence of past cyber attacks on DCS systems – which may be unnoticed due to lack of security measures or unreported due to concerns of plant owner/operators
- Potential vulnerabilities of power plant DCS systems
- Availability of tools and strategies to mitigate the risk

With regard to the first area, a number of such attacks on control systems in the electric power industry have been reported. For example, a March 2004 General Accounting Office (GAO) report on "Challenges and Efforts to Secure Control Systems" summarized such attacks, including a computer system breach at the Salt River Project as early as 1994. A Microsoft SQL Server worm known as "Slammer" disabled a safety monitoring system for several hours at the Davis-Besse nuclear power plant in Ohio in late 2003[1]. These attacks, though relatively minor in scope and damages, illustrate the potential for malicious cyber activity in the control networks or systems of the electric power industry.

DCS potential vulnerabilities

Recognizing the critical need for increased security of DCS networks and systems, Symantec is working with DCS industry leaders to define more specifically the types of vulnerabilities that exist in DCS systems. The pattern detected in these vulnerabilities is that most involve the potential for penetration of the DCS by attackers via another connected network or access point, with potential adverse financial and safety consequences. More specifically, Symantec and its partner have identified the following key potential vulnerabilities relevant to DCS systems:

- Intruders gaining unauthorized access to the DCS via overlooked key access points (e.g., via dial-up remote network access, or connections to contactor networks that are not secured, see Figure 2).
- Disgruntled employees posing a wide range of threats (e.g., authorization violation, in which an authorized user gains access to the DCS via the corporate network for an unauthorized purpose, see Figure 3).
- An intruder initiating a denial-of-service attack by sending repeated information requests that "lock up" a DCS server, preventing the server from performing legitimate operations and serving legitimate users.
- Viruses or worms infecting the DCS servers or other devices, and performing malicious activities such as emailing critical information to another host for retrieval by an attacker.
- In rare cases, well-intentioned employees or contractors inadvertently causing disruptions due to use of improper procedures or lack of preventive procedures to avoid these disruptions.

While this is not a comprehensive list of vulnerabilities, it serves to illustrate the type of vulnerabilities that could be exploited to a malicious end.

Effective practices for securing DCSs

Effective practices for protecting DCSs against these vulnerabilities can be grouped according to the four-step cyber security process shown in Figure 4.

The security assessment step includes gathering knowledge about the environment, both inside and outside of the organization. This includes awareness of electronic threats before they reach the organization, identifying possible regulatory compliance issues, assessing the effectiveness of security and administration tools, and manually validating these security concerns using penetration testing methods.

Security policy creation and enforcement establishes who is authorized to gain access to what information, establishes who is authorized to perform what functions, measures compliance with these policies and procedures, and recommends ways to improve compliance.

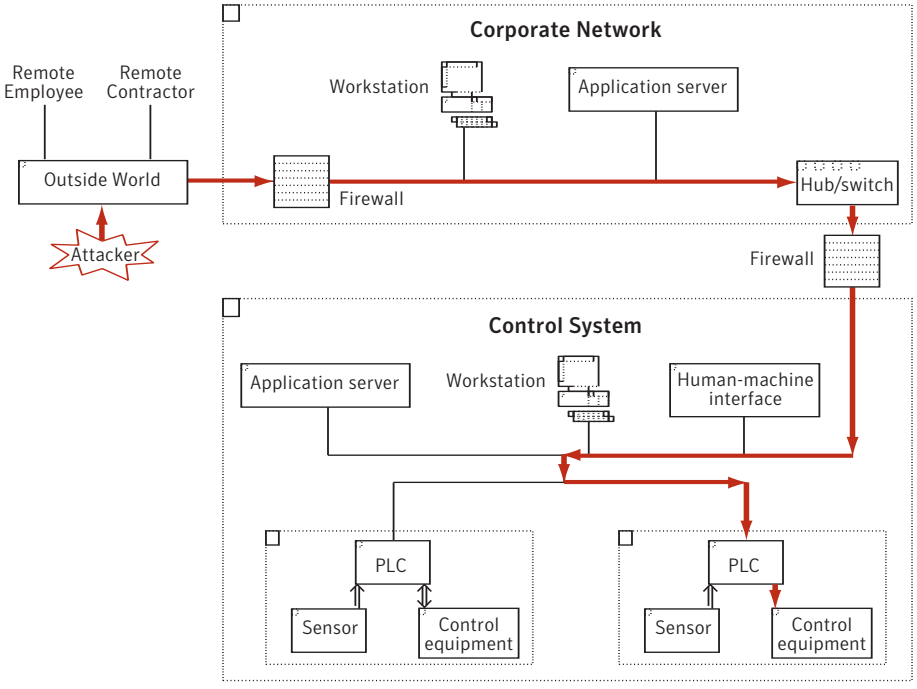

Figure 2
One vulnerability path involves remote access to the DCS

Security measure deployment includes the deploying of security measures and responding successfully to vulnerabilities; securing devices, applications, and networks against threats

before they occur; and taking steps to ensure that information is up-to-date, compliant, and restorable. It also involves recovery procedures and tools in the event that an attack eludes other security measures.

Security monitoring and management involves real-time, 24/7 monitoring and management of security information resources to prevent disruptions and minimize downtime.

Security assessments

The cyber security process begins with the assessment of the vulnerabilities of DCS networks and systems on a recurring basis. This activity is required under section 002 (identifying critical cyber assets) of the NERC CIP, as well as requirement 4 under section 005 (cyber vulnerability assessment for perimeter security) and requirement 9 under section 007 (cyber vulnerability assessment for security within the perimeter). The latter section, for example, requires that "responsible entities perform a cyber vulnerability assessment of cyber assets within the electronic security perimeter at least annually[2]."

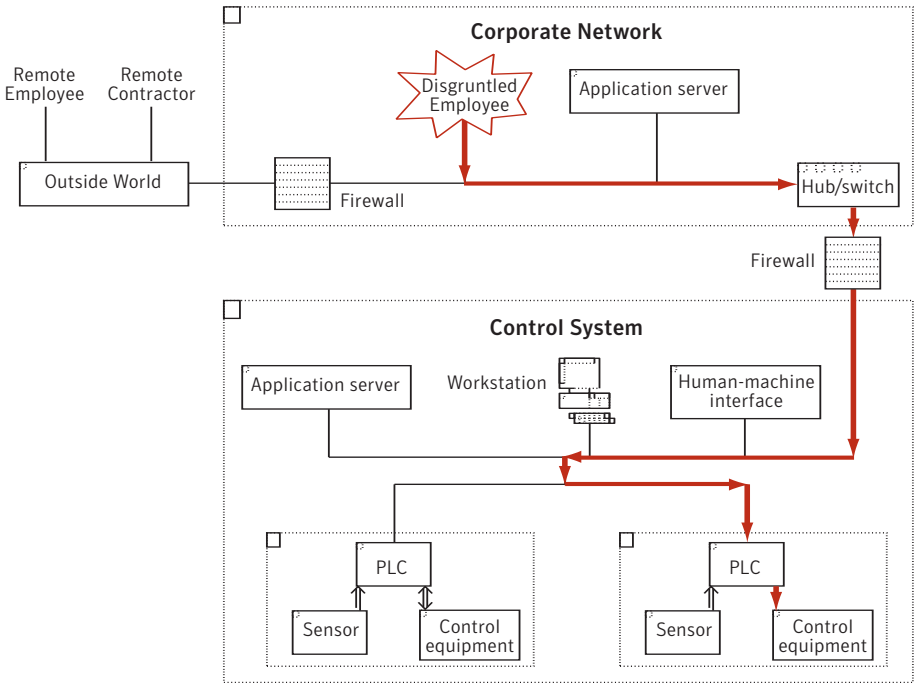

Figure 3
A second vulnerability path involves access to the DCS via the corporate network.

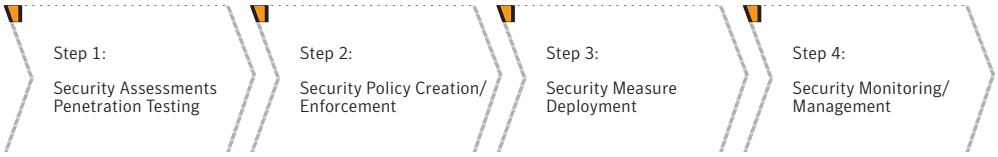

Figure 4
Four Critical Steps in the Cyber Security Process

Such security and risk assessment is complicated by the multiple DCS systems in place at most plants. Another complexity involves the interconnection of corporate networks and control networks; each type of network exposes a unique set of vulnerabilities, all of which must be assessed. Hence, corporate networks, Web servers, and customer management systems should also be assessed to reveal unintended gaps in security, including unknown links between public and private networks, and access control violations.

One key part of security assessment is penetration testing. The “always on” nature of control networks complicates such testing. This effectively rules out use of traditional IT security assessment companies with little or no experience conducting penetration testing in DCS environments.

An overwhelming number of security technologies, networking devices, and configuration options are available to power generation companies. While firewalls, intrusion detection systems, virtual private networks, and other technologies can all help protect control networks from malicious attacks, improper configuration and/or measures that are not tested and validated in the DCS environment can seriously hamper the effectiveness of any security posture.

Due to this complexity, and the often overtaxed nature of plant operators and other IT personnel, many power generation companies are likely to benefit from the services of independent consultants in this area. Such independent assessments can help ensure that evolving DCS and corporate network architectures do not compromise network security, while addressing vulnerabilities such as attacker attempts to bypass controls, attempted denial-of-service attacks, and many others.

Security policy creation and enforcement

The foundation of effective security effective practices is a comprehensive, well-conceived security policy. This activity is required under requirement 1 of section 003 (cyber security policy) of the NERC CIP. This section requires that “responsible entities document and

implement a cyber security policy that defines a structure of relationships and decision-making processes that identify and represent management's commitment and ability to secure its critical cyber assets[2]."

For the control systems used by power plant operators, security policies must address issues of who is authorized to gain access to what information, and who is authorized to perform what functions, as well as procedures that authorized parties must follow to ensure effective security. Such policies are particularly important for the control of access by parties outside of the power plant control room (e.g., employees accessing information via the corporate network, on-site and off-site contractors, remote employees, and others).

After establishing security policies, power generation companies need a policy compliance tool that measures the current state of security, compares it with the state needed to comply with regulations (e.g., NERC CIP) and company policy, and recommends measures to accomplish such compliance.

Security measurement deployment: firewalls are not enough

Taking action to respond to vulnerabilities and proactively securing networks and systems requires much more than implementing firewalls. Many power generation companies deploy perimeter firewalls to control the traffic entering and leaving their networks, thereby providing a first line of defense against external attacks. Another common measure is the deployment of firewalls between the corporate and control networks. Some security administrators believe that these firewalls provide sufficient protection across the company. However, firewalls can offer a false sense of security. Many firewalls simply allow or disallow certain types of traffic at each port. In order to secure these ports, companies need more than a firewall – they need security measures that recognize anomalies in IP traffic. These measures would ideally have vulnerability signatures for these specific protocols, which would trigger alarms if these vulnerabilities are exploited.

Another major reason that firewalls alone do not offer sufficient protection is that the network perimeter is no longer easily discernable. Companies once clearly defined "insiders" from "outsiders"; now power plant control centers must enable collaboration and open communication with contractors, remote employees, and others. Thus, attacks can be either unknowingly or maliciously perpetrated by those with legitimate network access. In fact, according to a recent CSI/FBI Computer Crime and Security Survey, one-third of network attacks are perpetrated by those inside the traditional firewall. Attacks could include integrity violations (i.e., unauthorized information creation or modification), authorization violations (in which an

authorized user gains access for an unauthorized purpose), intercept/alter (in which a packet is intercepted, modified, and forwarded), eavesdropping (i.e., data confidentiality is compromised via monitoring), and others.

Traditional firewalls also cannot protect against blended threats (i.e., threats that combine characteristics of hacking, denial-of-service attacks, and worm propagation). According to the Symantec Internet Security Threat Report issued in March 2004, blended threats represented 54 percent of the top ten submissions during the second half of 2003[3]. Traditional firewalls can even become the launch point for an attack.

Power generation companies need a solution at the network gateway that employs more than firewall technology. Perimeter security is required under section 005 of the NERC CIP, which "requires the identification and protection of the electronic security perimeter inside which all critical cyber assets reside, as well as all access points on the perimeter[2]." To meet these needs, effective practices should include the following at the network gateway:

- Purchasing separate firewall, intrusion detection, and antivirus technologies from different vendors can be costly to purchase, deploy, and update. In light of the limited IT resources in some DCS environments, Symantec recommends purchase of an integrated solution that combines all of these capabilities into a comprehensive gateway solution.
- The firewall solution should include both stateful inspection and full application inspection – a "hybrid" firewall.
- Due to the multiple protocols used in the DCS environment, the intrusion detection device should use both anomaly-based protection and signature-based protection.
- The antivirus solution should scan for at least 60,000 viruses and provide proactive protection via both signature-based and heuristics-based scanning. The antivirus solution is best deployed at the gateway, to minimize performance impact and facilitate updates.
- A solution that has received a high Evaluation Assurance Level (EAL), such as EAL level 4 or higher, is recommended.

Security measure deployment: network security

As a complement to the gateway security described above, power generation companies also need network security. This activity will help to address section 007 of the NERC CIP, which requires "responsible entities to have system security controls in force to detect, deter, and prevent the failure or compromise of critical function performed by critical cyber assets caused

by mistake, misuse, or malicious activity. This standard requires responsible entities to define methods, processes, and procedures for securing those systems determined to be critical cyber assets, as well as non-critical cyber assets within the electronic security perimeter."[2]

Security monitoring and management

As electric utilities deploy security technologies throughout their networks, the challenge of properly managing and monitoring these resources is becoming increasingly complex. Yet, such managing and monitoring is required under NERC CIP. For example, requirement 3 under section 005 requires "responsible entities to implement and document the controls for logging authorized access, detecting unauthorized access (intrusions), and attempts at unauthorized access at access points to the electronic security perimeter twenty-four hours a day, seven days a week." Similarly, requirement 7 of section 007 requires "responsible entities to ensure all cyber assets within the electronic security perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security."[2]

The implementation of "technology-only" solutions without close monitoring and management significantly weakens the effectiveness of security devices. Hiring experienced IT security professionals to monitor network security devices can help to mitigate risk; however, this option is cost-prohibitive for most, if not all, power generation companies. Additionally, most IT teams do not work seven days per week, 24 hours per day, which is a requirement in the utilities space. At the same time, power plant control center personnel must focus on their system operation duties and are typically not trained in the nuances of effective security monitoring and management. As a result, many organizations are using third parties that have experience in providing 24x7 management and monitoring of security devices to highly-specialized, managed security companies in the electric utilities environment.

Symantec solutions

For reference, Table 1 includes a summary of the recommended effective practices described in this paper, maps these practices to specific portions of the NERC CIP, and lists relevant Symantec products and services. Figure 5 illustrates potential locations for implementation of various Symantec solutions on power generation corporate and DCS networks.

Table 1. Summary of Recommended Effective Practices to Secure Power Plant DCSs

Effective Practice	Relevant NERC CIP Section	Symantec Offerings	Symantec Solution Description
Security Assessments			
Vulnerability Assessment	Section 002; R4 of Section 005; R9 of Section 007	Symantec SCADA / DCS Security Assessment Services	Symantec provides DCS security and risk assessment services, corporate network vulnerability assessments, incident forensics, and penetration testing to help customers in the electric power sector develop more robust information security infrastructures, processes, and programs.
Security Policy Creation and Enforcement			
Policy Creation and Enforcement	R1 of Section 003	Symantec Consulting Services Symantec Enterprise Security Manager™ (ESM)	Symantec ESM provides comprehensive, policy-based security assessment and management. Using templates based on the NERC standards and Sarbanes-Oxley, it provides a solid foundation for power generation companies to begin implementing the NERC standards and measure their ability to adhere to the standards.
Security Measure Deployment			
Beyond Firewalls: Integrated Gateway Security	Section 005	Symantec™ Gateway Security (SGS)	Symantec SGS includes full-inspection firewall technology, protocol anomaly-based intrusion prevention and intrusion detection engines, award-winning virus protection, URL-based content filtering, anti-spam technology, and IPSec-compliant virtual private networking technology with hardware-assisted high-speed encryption. This appliance provides strong security at the gateway between the Internet and the corporate network or control network, or between network segments.
Network Security	Section 007	Symantec™ Network Security (SNS)	Symantec SNS provides proactive intrusion protection against known and unknown attacks to secure critical networks. It combines protocol anomaly, signature, statistical, and vulnerability attack interception techniques to accurately identify and block known or unknown (zero-day) attacks and worms from spreading throughout networks.

Table 1. Summary of Recommended Effective Practices to Secure Power Plant DCSs (continued)

Security Monitoring and Management			
Managed Services	R3 of Section 005; R7 of Section 007	Symantec ™ Managed Security Services	Symantec currently manages the security infrastructures of several leading U.S. electric utilities. This service provides 24/7 centralized management and monitoring of protection technologies along with early warnings, incident response, and decision support. The services ensure that all security devices are configured properly and fully patched, and monitor the actual activity on each device to detect malicious activity in real time.

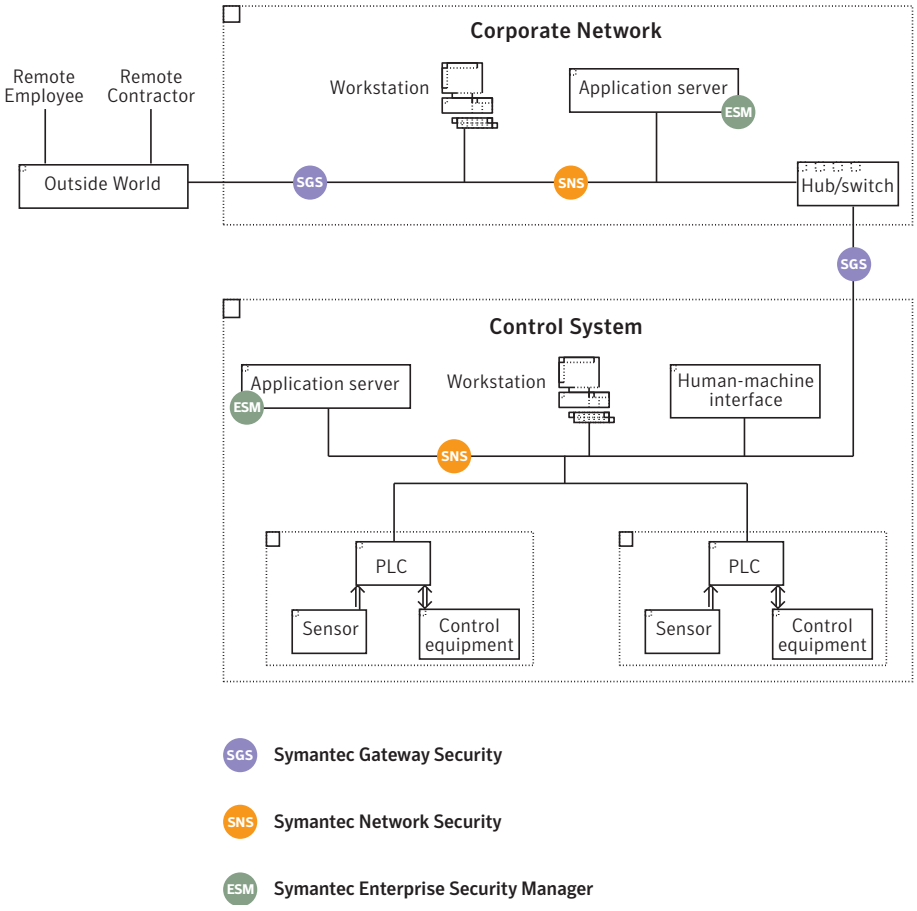

Figure 5
In this conceptual diagram, Symantec solutions enable power generation companies to implement recommended effective practices for securing DCSs.

References

1) United States General Accounting Office, Report to Congressional Requesters, "Critical Infrastructure Protection, Challenges and Efforts to Secure Control Systems," GAO-04-354, March 2004.

2) NERC CIP Cyber Security Standard, Draft 3: May 9, 2005, ftp://www.nerc.com/pub/sys/all_updl/standards/sar/CIP002-CIP009_Draft3.pdf.

3) Symantec Corporation, "Symantec Internet Security Threat Report," Trends for July 1, 2003 – December 31, 2003, Volume V, published March 2004.

About Symantec

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 800 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
408 517 8000
800 721 3934
www.symantec.com

07/05 10439569