White Paper

Honeywell

Honeywell Process Solutions

Security Solutions to Meet NERC-CIP Requirements

Kevin Staggs, Honeywell Process Solutions

Table of Contents

Introduction **3**

Nerc Standards and Implications **3**

How to Meet the New Requirements **4**

Protecting Your System **4**

Cyber Security 5

A Sample Power Plant Implementation **6**

Conclusion **9**

References **9**

Table of Figures

Figure 1 – ISA99 Levels of Control **7**

Figure 2 – High Security Network Architecture **8**

Introduction

As deadlines for the North American Electric Reliability Council Critical Infrastructure Protection (NERC-CIP) standards approach, power plants and electric utilities must begin implementing the necessary security practices to meet the compliance requirements. This paper will address the NERC-CIP standards and how Honeywell solutions can increase plant safety and meet these critical reliability guidelines.

Background

In the process and manufacturing industries, the advent of open architectures and standard protocols presents both new opportunities and risks for plant enterprises. While the evolution from isolated proprietary applications to open technology has expanded business information availability, it has also exposed the enterprise to electronic threats.

Most process control systems used today were not originally designed to defend against cyber attacks. The events of 9/11 and recent cyber incidents on control systems have increased awareness of the inherent vulnerabilities of control systems connected to the Internet and remote telephone connections.

Recently, the Federal Energy Regulatory Commission (FERC) approved eight new mandatory critical infrastructure protection (CIP) reliability standards designed to protect the nation's bulk power system against potential disruptions from cyber security breaches. The reliability standards were developed by the North American Electric Reliability Corporation (NERC), which FERC has designated as the electric reliability organization (ERO).

Nerc Standards and Implications

In June 2006, NERC adopted Cyber Security Standards CIP-002 through 009 specifying the minimum requirements needed to ensure the security of the electronic exchange of information for supporting the bulk power system. NERC-CIP identifies standards in key areas designed to protect power plants and all other aspects of electric utility operations and assets. The standards include provisions for identifying critical cyber assets, developing security management controls, training, perimeter and physical security, incident reporting and response planning, and recovery plans.

FERC, in its Notice Of Proposed Rulemaking (NOPR) released July 20, 2007, has proposed to approve these standards, with directed modifications, as mandatory and enforceable with significant sanctions and penalties of up to $1 million per day for utilities found to be noncompliant.

According to the NERC-CIP implementation guidelines, companies must be substantially compliant by December 31, 2008, compliant by December 31, 2009, and auditably compliant by December 31, 2010.

Many electric utilities are unsure how to deal with NERC-CIP regulations. Some power companies are struggling to establish a direction or are taking a "wait and see" approach until there is more clarity around the still evolving regulations.

NERC-CIP establishes standards in eight key areas designed to protect not only power plants, but all other aspects of electric utility operations and assets as well. The standard includes provisions for identifying critical cyber assets (section 002), developing security management controls (section 003), implementing training (section 004), identifying and implementing perimeter security (section 005), implementing a physical security program for the protection of critical cyber assets (section 006), 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).

These eight standards address the same areas covered by the NERC 1200 Standard, adopted in 2003, but with some important differences. For example, instead of requiring organizations to identify their critical cyber assets directly, they must now identify their

critical assets and then determine their critical cyber assets. (A critical cyber asset must be dial-up accessible or use a routable protocol for communication.)

In many ways, CIP-002 through CIP-009 set a higher bar for security. While the standard has not been finalized and may be modified, deployment of security best practices will help to address the requirements in a phased manner without requiring a one-time, major investment.

How to Meet the New Requirements

Security improvements should be part of an enterprise-wide risk management program for all process and manufacturing companies, but the challenges are daunting. Moreover, the two groups 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 of the serious problem slows progress.

Process and manufacturing companies need a comprehensive security strategy addressing process, people and technology. Honeywell's strategy includes assessment of all cyber related assets, analysis of risk, design of mitigation strategies and implementation of those strategies, and monitoring/management of the entire security strategy, in order to ensure the security of critical assets. It also employs strong defensive technologies such as patch management, anti-virus software, intrusion detection and security monitoring. All personnel must understand their role in maintaining the security of plant systems.

A successful and effective plant safety and security solution begins with a strategy incorporating security at all levels of the operation. It is important to keep control systems and networks current with security updates, security procedures, documented best practices, regular assessments and testing.

The first step in meeting the NERC-CIP requirements is a security assessment, which involves 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 processes, and manually validating these security concerns using penetration testing methods where it is safe to do so.

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

Deployment includes design and implementation 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 an attack eludes other security measures.

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

Protecting Your System

A dramatic transformation from proprietary to open control systems is underway within the process industry. This trend, coupled with the connectivity between open control systems and enterprise networks, has introduced unprecedented cyber vulnerabilities in control systems.

Without an effective cyber security regimen, the fundamental mission of process control – to ensure safe and reliable operations – can be compromised by an ordinary cyber threat. Therefore, a comprehensive cyber security policy is an essential element of every process control and safety system implementation.

Honeywell advocates a layered approach to seamlessly integrate multiple technologies as the most secure way to protect a plant's people and assets, incorporating security at all levels from the process control network to the perimeter of the plant. At the core of this sphere of protection is process design, ensuring that processes are controlled by a secure process control network (PCN) extending across the entire plant and business networks.

Layers of protection include managing assets to ensure that the process design continues to function as intended, while protecting the plant from pending incidents with an early indication of failing assets. An integrated approach implements tools and procedures for managing abnormal situations and reducing incidents. When an abnormal situation occurs, alarm management solutions help ensure that operators have the information they need in the context they need it. This allows operators to react to situations quickly and accurately, thereby avoiding or mitigating safety incidents.

Next, properly designed emergency shutdown systems and automated procedures can move a plant to a safe state in the event an incident escalates beyond the inner layers of this sphere of protection. Should an incident occur, fire and gas detection solutions, coupled with rapid location of individuals and a carefully designed emergency response procedure, will help contain the impact.

Honeywell's layered solution also protects the perimeter of the facility using access control, asset tracking, perimeter detection and video surveillance.

Cyber Security

Plants should start with a site vulnerability assessment aimed at creating layers of protection from the control network through the perimeter of the plant. Deep understanding of site vulnerabilities is essential before users can take intelligent action to remove or mitigate associated security risks and establish comprehensive layers of protection.

The subject of cyber security is of particular importance to industries that are reliant on process control systems. Management must understand the difference between protecting facilities and data, and protecting processes operated or controlled with information technology. Security measures appropriate for traditional IT data networks could be disastrous if inappropriately applied to process control systems resulting in damage to productivity, capital assets and possibly human life.

An effective cyber security plan should include regular risk and vulnerability assessments, hierarchical networks with access restrictions at each level, high-security model deployed on personal computers and servers, physically separated process control and enterprise networks with limited access points, security hotfix and an antivirus deployment strategy; and disaster recovery.

In addition to properly managing cyber security, it is important to prepare for the possibility of a disaster that could impact critical data. Even a simple hardware failure could seriously jeopardize critical data, and therefore data recovery plans must be in place and allow for rapid recovery through an automated backup and restore application.

With open technology platforms, control system networks in power plants are exposed to the same security threats facing corporate networks, but with the added safety considerations associated with the process industries. These threats include:

- Indiscriminant, potentially destructive intrusions, such as viruses and worms
- Network spoofing and denial of service attacks that have performance impacts and potential safety issues
- Eavesdropping and password cracking that are threats to confidentiality
- Malicious threats, such as data tampering, impersonation and packet modification

Corporate IT groups manage these issues and challenges for enterprise networks. However, specialized skills are required for process control management processes, services and tools.

To help process companies cope with an increasingly complex open technology environment and resulting security issues, automation suppliers have developed IT service solutions focused on optimizing plant security measures. These services deploy certified network architects and specialists with expertise in industrial networking and an in-depth knowledge of process automation systems. This combination of skills is essential in assessing, designing, implementing and managing the PCN.

Whether identifying cyber assets or pinpointing cyber risks and recommended mitigations, companies can benefit from outsourcing process IT using the same methodologies their corporate IT group uses for outsourcing. Process IT outsourcing is a cost-effective alternative to maintaining an in-house IT capability and can help keep process control networks running in a secure environment.

By partnering with their automation supplier, companies can implement a sound PCN security policy focusing on the preservation of confidentiality, integrity of data and network availability. A network security assessment establishes a baseline of the current security processes, procedures and safeguards used to protect a process control network from external threats. This baseline can be used to create a documented set of recommendations outlining procedures and changes to the environment that will mitigate identified vulnerabilities.

The PCN security design process provides a detailed design of the security infrastructure connecting a process control network to a company's plant information network. Initial steps in the design process include an analysis of security requirements, including adherence to policies and regulations.

The automation supplier, from a secure remote services center, can also deliver PCN security management services. These services are often combined with on-site vendor or plant personnel to create a comprehensive security management solution.

A Sample Power Plant Implementation

To assist with the understanding of how the NERC-CIP standards can be met, this section will define an implementation of a sample power plant system configuration. This sample power plant system configuration is based upon the emerging ISA SP99 standard. The ISA SP99 standard is a cyber security standard for manufacturing and control systems. The definition for the ISA SP99 committee work from the ISA web site is as follows: "The ISA99 Committee will establish standards, recommended practices, technical reports and related information that will define procedures for implementing electronically secure manufacturing and control systems and security practices and assessing electronic security performance. Guidance is directed towards those responsible for designing, implementing or managing manufacturing and control systems and shall also apply to users, system integrators, security practitioners, and control systems manufacturers and vendors."[4]

The ISA99 Committee has already published part 1 of the standard. This section of the standard is titled *Security for Industrial Automation and Control Systems: Concepts, Terminology and Models*. Part 2 of the standard is currently in the voting process and is titled *Establishing an Industrial Automation and Control Systems Security Program.* Part 2 of the standard when followed will allow an end user to meet the requirements of the NERC-CIP standards. Also underway is work to develop a Part 4 standard, *Technical Requirements for Industrial Automation and Control Systems*, and to develop a technical report on patch management.[4]

There is enough of the standard published to begin implementing a cyber security program and meet the requirements of NERC-CIP. Following is an example power plant configuration based upon the standards and some level of detail for an implementation that will meet the standard.

The ISA SP99 committee has identified a layered structure for manufacturing and control systems. This layered structure is shown in Figure 1 below. In this diagram the control system is compartmentalized into functional layers of control with the lowest levels being the process valves, actuators and sensors and the protective system. Moving up to the next level are the controllers connected to the process which is titled Basic Process Control. This level of control is intended to be able to control the system without human interaction. Above the Basic Process Control level is the Area Supervisor Control level, the first level where the HMI interface is

introduced. The next level up is Site Manufacturing Operations where traditionally the entire plant is connected together. The next level up is Site Business Planning, the first level where the IT and security management of the system is done by the traditional IT organization. Levels 3 and below comprise the manufacturing and process control system. The attention of the ISA99 committee is focused on these levels and this power plant example will do likewise.

The system at Level 3 and below has a different management philosophy than that of traditional IT systems. Since the primary purpose of a manufacturing and control system is to make products around the clock, availability is a primary security attribute of the control system. This drives a different security management process for the manufacturing and control system. Because of this there is a standard practice to install a firewall between the level 3 and level 4 networks.

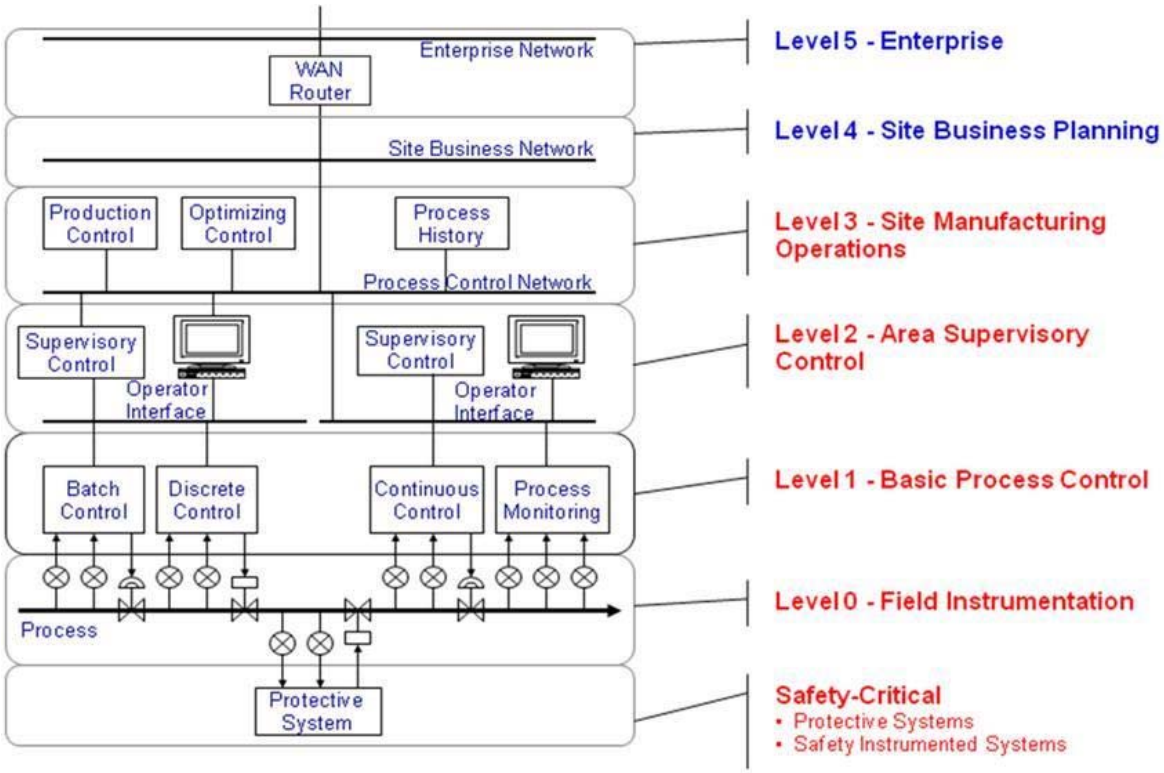

Figure 1 – ISA99 Levels of Control

Figure 2 below shows a system implemented that follows the ISA99 levels of control and provides additional system management components that will help end users comply with NERC-CIP.

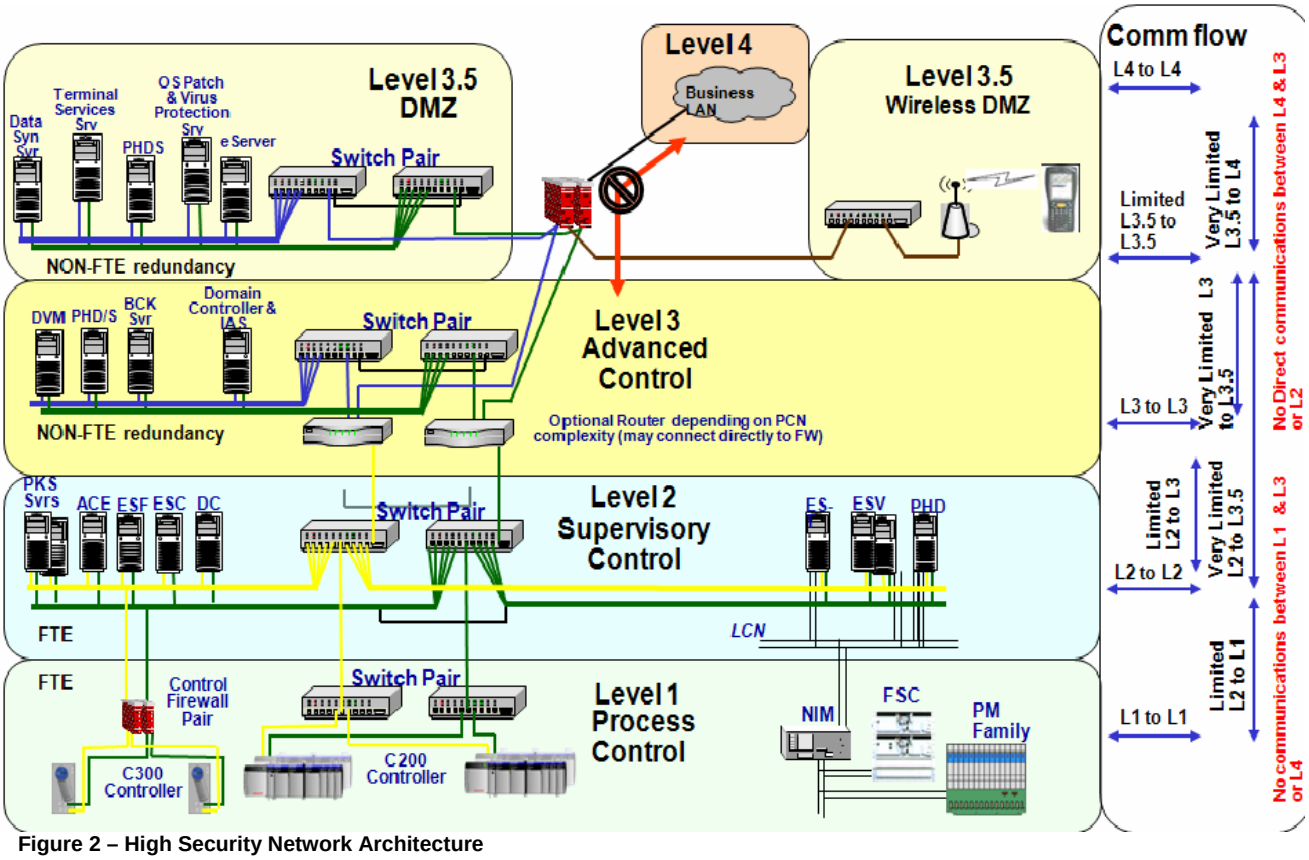

Figure 2 – High Security Network Architecture

The High Security Network Architecture will meet the CIP-005 requirements and help with the conformance to CIP-007. CIP-005 is met by segmenting the system into levels as defined by the ISA99 standard. In Figure 2, the network is partitioned into network levels creating security perimeters in the system. This first security perimeter is created with the firewall which is located between Level 3, Level 4 and the Level 3.5 DMZ. There is an addition in this conceptual implementation showing the Level 3.5 DMZ. The purpose of the DMZ is to provide an additional security zone and also an area for the data servers which move the data between the systems at level 3 and level 4. In the diagram above, a historian is located in the DMZ to achieve data movement and it is possible to provide a view of the process through the DMZ without having to log on to the process control system. The diagram above adds an additional security perimeter between level 2 and level 3 by providing a set of routers that limit the communications between the two levels. The communication flow on the right side of the diagram shows how network traffic is restricted between the various network levels creating security perimeters in the system.

The diagram provides a configuration which will meet the requirements of CIP-007 for Systems Security Management, including anti virus software and security updates. To meet these requirements there must be servers that provide the updates to the nodes at level 3 and below. These servers are shown in the DMZ as the OS Patch and Virus Protection Server. This server is providing the updates necessary to the manufacturing and control system below it at level 3. The updates are obtained from update servers that are located in the company's IT network providing updates for those systems. A separate server is required so that the deployment of the updates can be managed by the process control team rather that the corporate IT team. This is required so that the deployment of updates onto the control system in the power plant can be scheduled and deployed to the system at a time when it is safe to do so.

CIP-009 requires that recovery plans for the process control system be in place. Part of creating recovery plans is to document and test the backup and recovery processes for the control system. Most backup programs today are not capable of backing up locked files and most control systems today lock critical files as part of their normal operation. Most IT backup systems will take the IT subsystem off-line for a period of time in order to perform the backup. It is important to ask you control system vendor to provide a backup subsystem which will provide the necessary functionality for backing up a process control system on-line.

One final area in the fictitious power plant is a strategy for meeting the CIP-006 Physical Security Standard. This requirement can not be met directly with the control system but integrating this information into the control system can provide for a higher level of safety at the power plant. The physical security system will be able to:

- Identify and control who enters and exits the facility
- Track movements of building occupants and assets
- Control access to restricted areas
- Track and locate equipment, products and other resources
- Track the location of personnel on site in the event of an incident
- Integrate control and security systems for greater speed and efficiency
- Respond proactively to alarms and events

There is an advantage to integrating the physical security and process control systems together to provide a common alarms and events structure. Process operators may need to know about physical security alerts. For example, if an unauthorized person has entered a critical process area the process operator may need to take action to protect the plant or the person from damage. For example, when a process area like a steam plant is starting up, the process operator needs to know that all personnel are clear of the area. Having the systems integrated allows for the operators to know this. It may also be beneficial for plant security personnel to know about certain types of process or plant upsets. The benefits of integrated physical security and process control are documented in a white paper that can be read at: http://hpsweb.honeywell.com/Cultures/en-US/NewsEvents/SuccessStories/success_geismar.htm

Conclusion

The impending NERC-CIP standards are forcing significant changes in the utility networking and computing infrastructure. Companies can look at cyber security as merely an intrusive requirement, forcing investment in security-specific technologies, or alternatively, they can view this as an upgrade to their infrastructure that creates opportunity for much broader improvements and benefits.

References

1. http://csrp.inl.gov/documents/MitigationsForVulnerabilitiesCSNetsISA.pdf

2. SHAW, J., “NERC/CIP Compliance: Headache or Opportunity,” Utility Automation & Engineering, (July 2007)

3. LINDSTROM, J., “Inside the NERC CIP Standards,” (Sept. 2005), http://www.symantec.com/business/library/article.jsp?aid=IN_091105_inside_nerc_cip_standards

4.http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821

For More Information

For more information about Security Solutions to Meet NERC-CIP Requirements, visit our website at www.honeywell.com/ps or contact your Honeywell account manager.

Automation & Control Solutions
Process Solutions
Honeywell
2500 W. Union Hills Dr.
Phoenix, AZ 85027
Tel: 877.466.3993 or 602.313.6665
www.honeywell.com/ps

WP-08-22-ENG
July 2008
Printed in USA

Honeywell