Proceedings of the ISA Expo, Chicago, IL, October 25 - 27, 2005.

NIST Industrial Control System Security Activities

Keith Stouffer
Mechanical Engineer
National Institute of Standards & Technology
Gaithersburg, MD 20899

KEYWORDS

Security, Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS), Process Control Security Requirements Forum (PCSRF), Industrial Control Systems (ICS)

ABSTRACT

The National Institute of Standards and Technology (NIST) has several ongoing efforts to address industrial control system security. This paper will present an overview of two of these efforts, the Process Control Security Requirements Forum (PCSRF) and the upcoming Special Publication 800-82.

The Process Control Security Requirements Forum (PCSRF), formed in spring of 2001, is a 650 member working group of users, vendors, and integrators in the process control industry which is addressing the cyber security requirements for new industrial process control systems and components, including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), and Intelligent Electronic Devices (IEDs).

NIST Special Publication 800-82, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security*, scheduled for release in January 2006, provides guidance for establishing secure SCADA and Industrial Control Systems. The document provides an industrial control system overview and typical system topologies to facilitate the understanding of industrial control systems, identifies typical vulnerabilities and threats to these systems and provides recommended security countermeasures to mitigate the associated risks.

INTRODUCTION

The National Institute of Standards and Technology (NIST) is working with process control end users, vendors and integrators to improve the Information Technology (IT) security of networked digital control systems used in industrial applications. The widespread use of IT for remote monitoring and control of the electric power system and for controlling industrial processes in the oil and gas, water, chemical, pharmaceutical, food and beverage, pulp and paper, and other industries, has unintentionally introduced security vulnerabilities. These systems are time critical and were designed to maximize performance, reliability and safety. Security had not been a significant consideration because these systems were often air-gapped from any other network and have been based on proprietary hardware and protocols. This has often been called security through obscurity. But today, these process control systems are often connected to the business networks to allow business personnel to make decisions, and they are also making greater use of commercial off the shelf products and open protocols.

PROCESS CONTROL SECURITY REQUIREMENTS FORUM (PCSRF)

To address the security requirements for industrial process control systems and components, NIST formed the Process Control Security Requirements Forum (PCSRF) [1] in the spring of 2001. The NIST-led PCSRF is a working group of users, vendors, and integrators in the process control industry which is addressing the cyber security requirements for new industrial process control systems and components, including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), and Intelligent Electronic Devices (IEDs). Members of the PCSRF represent the critical infrastructures and related process industries, including oil and gas, water, electric power, chemicals, pharmaceuticals, metals and mining, and pulp and paper. There are currently over 650 members, from 32 countries in the PCSRF representing government, academic and private sectors.

The main goal of the PCSRF is to increase the security of industrial process control systems through the definition and application of a common set of information security requirements for these systems. This will reduce the likelihood of successful cyber-attack on the nation’s critical infrastructures. One example of what PCSRF is trying to protect is the operator interface for the control system. The data that is displayed on the operator interface could be coming from sensors and devices many miles away. If this data became compromised, what the operator sees on the screen may not reflect what is really happening. This may cause the operator to take an action, such as flipping a breaker when it is not required, or it may cause the operator to think everything is normal and not take an action when an action is required. This could cause loss of production, generation or distribution. The Common Criteria for Information Technology Security Evaluation, also known as ISO/IEC 15408, is being used to document the results of this effort in the form of Protection Profile (PP) security specifications. The National Information Assurance Partnership (NIAP) maintains a repository of Protection Profiles [2].

SYSTEM PROTECTION PROFILE FOR INDUSTRIAL CONTROL SYSTEMS (SPP-ICS)

The PCSRF System Protection Profile for Industrial Control Systems (SPP-ICS) [3] is designed to present a cohesive, cross-industry set of security requirements for new industrial control systems. The security requirements specified in the SPP-ICS have been captured from approximately 10 face-to-face meetings of the PCSRF group and specific industry sectors as well as an additional 10 or so conference calls with the group over the past 3 years. The SPP-ICS is designed to be an industry voice to the industrial control system vendors and system integrators, defining the security capabilities that are desired in new products and systems. It is a consensus-based specification, not a NIST specification. These security requirements could be specified in procurement RFPs for new industrial control systems. There is no intent to suggest or imply that the Government will enforce the adaptation of these requirements. The SPP-ICS considers an entire system and addresses requirements for the entire system lifecycle. The SPP-ICS also acts as a starting point for more specific system protection profiles (SCADA, DCS, etc.), for a specific instance of an industrial control system (water, oil/gas, etc.), and for component protection profiles (industrial controller authentication, encryption modules, etc).

SCADA PROTECTION PROFILE

In March 2005, a PCSRF working group was created to take the next step and develop a SCADA PP. In the development of the SCADA PP, the security requirements defined by the group would be organized into sections that can be met by specific components and/or vendors. This will allow vendors to concentrate on the requirements that they can meet and develop a product for, rather than trying to decipher the big picture and determine what requirements they can address. This could provide a path for quicker vendor adoption and backing of the effort.

Soon after the first meeting of the working group, it was decided that a two PP approach would be used to develop the SCADA PP. A Control Center PP will specify the requirements for the SCADA Control Center and a Field Device PP will be developed to address the requirements for the field communications and devices. The two PPs will then be connected using the methodology defined in the Common Criteria. Figure 1 shows a high level diagram of the two PPs that create the SCADA PP.

Integrity and availability are two of the most important security issues for industrial control systems (ICS) and will be reflected in the Protection Profiles. Strong authentication of users, authentication of subjects, and authentication of data integrity in transit and at rest are required of all systems in the Target of Evaluation (TOE). A robust, yet flexible access control system is required that provides both role based and location based access control methods. The majority of the functional requirements address integrity issues. Availability is also extremely important for ICS, especially those that control critical infrastructures. While the functional requirements that address availability are smaller in number, they are robust as well. Confidentiality is often a lesser concern in most ICS. Functional requirements related to confidentiality deal primarily with TOE communication outside of a physical security boundary.

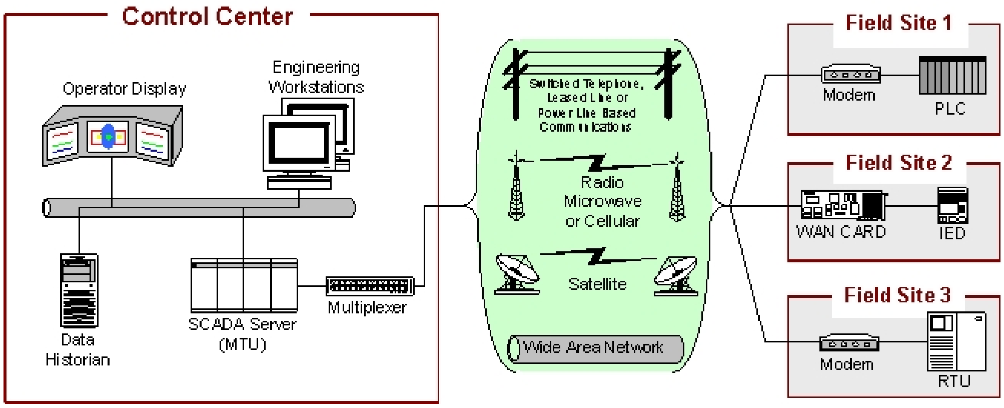

FIGURE 1. THE SCADA PP CONTAINS TWO CONNECTED PROTECTION PROFILES – CONTROL CENTER AND FIELD DEVICE

SCADA DEFINITION

The following is the SCADA system definition that was developed for the SCADA PP effort:

Supervisory Control and Data Acquisition (SCADA) systems integrate data acquisition systems with data transmission systems and Human-Machine Interface (HMI) software in order to provide a centralized monitor and control system for numerous process inputs and outputs. SCADA systems are designed to collect information, transfer it back to a central computer, and display the information to the operator(s) graphically or textually, thereby allowing the operator to monitor and/or control an entire system from a central location in real time. Based on the sophistication and setup of the individual system, control of any individual system, operation, or task can be automatic, or it can be initiated by operator commands.

SCADA systems are often used for electronic tagging of control and data points. Tags can include control inhibit, alarm and scan inhibit, as well as caution and informational messages as allowed in a utility's operational procedures.

SCADA systems consist of both hardware and software. Typical hardware includes a Master Terminal Unit (MTU) placed at a central location, communications equipment (radio, telephone line, cable or satellite), and one or more geographically distributed remote stations consisting of either a Remote Terminal Unit (RTU) or a Programmable Logic Controller (PLC), which controls actuators and/or monitors sensors. The MTU stores and processes the information from RTU inputs and outputs, while the RTU/PLC controls the local process. The communications hardware allows the transfer of information and data back and forth between the MTU and the RTUs/PLCs. The software is programmed to tell the system what and when to monitor, what parameter ranges are acceptable, and what response to initiate should the parameters go outside acceptable values. An Intelligent Electronic Device (IED), such as a protective relay, may communicate directly to the SCADA Master Station or a local RTU may poll the IEDs to collect the data and pass it to the SCADA Master Station. IEDs provide a direct interface to control and monitor equipment and sensors. IEDs can be directly polled and controlled by the SCADA Master Station and may have local programming that allows for the IED to act without direct instructions from the SCADA Master Station.

SCADA systems are used to control dispersed assets where centralized data acquisition is as important as control and are used in the distribution operations of water supply systems, oil/gas pipelines, electrical systems and rail systems.

CONTROL CENTER PROTECTION PROFILE

The Control Center Protection Profile [4] portion of the SCADA PP defines the minimum security requirements for an ICS Control Center used to control a critical infrastructure component. A Control Center typically includes real time servers, HMI stations for operators, historian servers, a network infrastructure, and any other management components that enable centralized control of the critical infrastructure. A Control Center is a central point for gathering information about the critical infrastructure system, that includes programs to analyze and present this information, and issues commands to modify the critical infrastructure system. A large, complex, and geographically dispersed infrastructure system can be operated by a small number of people in a Control Center.

The Control Center boundaries are both physical, such as a Control Center room, and logical. A logical boundary could include a Primary Control Center, Backup Control Center, and remote HMI stations. This Protection Profile defines the confidentiality, integrity, and availability requirements for information and communication while inside a physical and logically defined Control Center boundary. The Protection Profile also defines requirements for the import of data from PLCs, RTUs, and other field devices that are outside the TOE and addressed in the Field Device PP. At the time this paper was written, the requirements of the Control Center PP are in the process of being vetted by the PCSRF SCADA working group. Figure 2 shows the Control Center TOE and security perimeters.

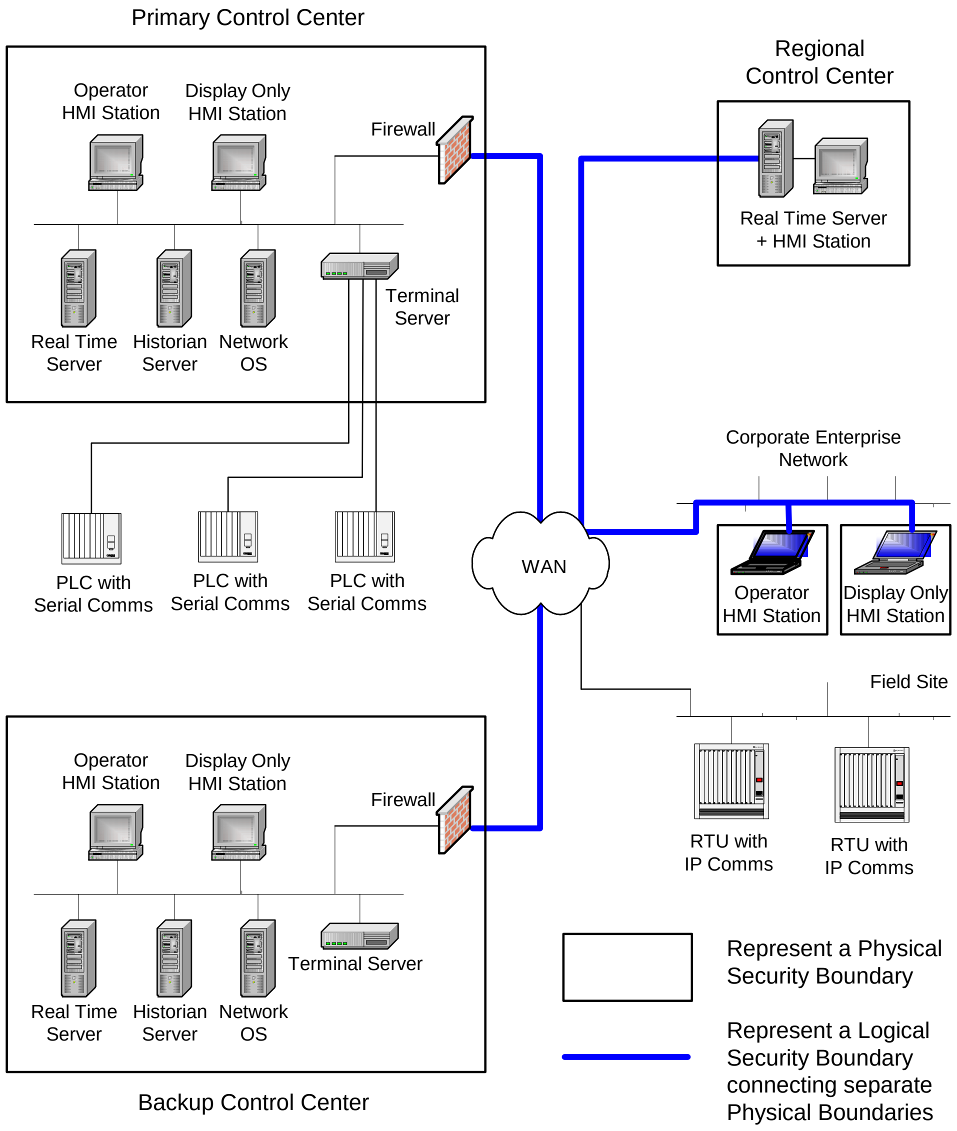

FIGURE 2. CONTROL CENTER TOE AND SECURITY PERIMETERS

FIELD DEVICE PROTECTION PROFILE

Most current SCADA field devices are highly insecure because encryption, authentication, and other security measures were not designed into the devices. An adversary could potentially exploit these insecurities by inserting false commands and responses, modifying legitimate communication, or altering field device behavior.

Common vulnerabilities in SCADA field devices include (but are not limited to):

- TCP/IP addressability
- Weak or nonexistent authentication
- Remote configuration capabilities and modem access
- Open FTP, Telnet, SNMP and HTML ports that allow for remote configuration
- Configuration modes that are protected by passwords sent in clear text
- Unencrypted communications with SCADA MTU
- Lack of configuration backups
- Embedded web servers
- Default OS security configurations
- Uncollected or unexamined system logs

Security capabilities don't exist in many current SCADA field devices largely because appropriate security solutions are not available. Vendors have not had a business case for developing SCADA field devices with security capabilities. This is why there is a need for a SCADA Field Device Protection Profile (PP). Concise functional and assurance security requirements need to be specified for new SCADA field devices so that the requirements can get into the product design cycle and the vendors have specific security requirements to build to. The Field Device PP is scheduled to begin development by October 2005 and be completed by May 2006.

NIST SPECIAL PUBLICATION 800-82

NIST is in the process of developing Special Publication (SP) 800-82, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security,* scheduled for release in January 2006. The purpose of SP 800-82 is to provide guidance for establishing secure SCADA and Industrial Control Systems. It provides an industrial control system overview and typical system topologies to facilitate the understanding of the unique requirements for industrial control systems, identifies typical vulnerabilities and threats to these systems and provides recommended security countermeasures to mitigate the associated risks. Readers are encouraged to tailor the recommended guidelines and solutions to meet their specific security and business requirements. Like all SP 800 documents, SP 800-82 will be available on the NIST Special Publications website [5].

The scope of SP 800-82 includes SCADA and Industrial Control Systems that are typically used in the electric, water, oil & gas, chemical, pharmaceutical, pulp & paper, food & beverage, and discrete manufacturing (automotive, aerospace and durable goods).

AUDIENCE

SP 800-82 covers details specific to SCADA and Industrial Control Systems and is technical is nature; however, it provides the necessary background to understand the topics that are discussed.

The following list documents how people from different backgrounds can use SP 800-82. The intended audience is varied and includes the following:

- Control engineers, integrators and architects when designing and implementing secure SCADA and/or industrial control systems
- System administrators, engineers and other IT professionals when administering, patching and securing SCADA and/or industrial control systems
- Security consultants when performing security assessments of SCADA and/or industrial control systems
- Managers responsible for SCADA and/or industrial control systems
- Researchers and analysts who are trying to understand the unique security requirements of SCADA and/or industrial control systems
- Vendors developing products that will be deployed in SCADA and/or industrial control systems

SCADA AND INDUSTRIAL CONTROL SYSTEMS OVERVIEW

The first major section of SP 800-82 provides an overview of SCADA and industrial control systems and their typical system topologies to facilitate the understanding of the unique requirements for industrial control systems. This section of SP 800-82 is meant to provide information to system administrators, engineers and other IT professionals when administering, patching and securing SCADA and/or industrial control systems. Information in this section includes the key differences between general IT systems and industrial control systems including performance requirements, reliability requirements, management requirements and security architectures. There is also a discussion on how the US critical infrastructure is often referred to as a “ system of systems” because of the interdependencies that exist between its various industrial sectors. Critical infrastructures are highly interconnected and mutually dependent in complex ways, both physically and through a host of information and communications technologies. What happens to one infrastructure can directly and indirectly affect other infrastructures through cascading and escalating failures.

SCADA AND INDUSTRIAL CONTROL SYSTEMS VULNERABILITIES

This section of SP 800-82 explains that most ICS in use today were developed years ago, long before public and private networks, desktop computing or the Internet were a common part of business operations. These systems were designed to meet performance, reliability, safety, and flexibility requirements and were typically physically isolated and based on proprietary hardware, software and communication protocols. These proprietary communication protocols, such as MODBUS, include basic error detection and correction capabilities, but nothing that guarantees secure communications. The need for cyber security measures within these systems was not anticipated, and at the time, security meant physically securing access to the network and the consoles that controlled the systems.

Over time, through the 1980's and 1990's, as microprocessor, Personal Computer and networking technology evolved, the design of SCADA and industrial control systems changed to incorporate the latest technologies. In the late 1990's and into the 2000's Internet-based technologies started making their way into ICS designs.

Today, several factors have contributed to the increased risk to control systems, including:

- Adoption of standardized protocols and technologies with known vulnerabilities
- Connectivity of the control systems to other networks
- Insecure and/or unknown remote connections
- Widespread availability of technical information about control systems

One of the most common vulnerabilities in modern SCADA and industrial control systems is the lack of a process control-specific security policy. Other vulnerabilities [6] include poor account maintenance, insecure network connections, and a lack of maintenance and monitoring of equipment.

INDUSTRIAL CONTROL SYSTEMS SECURITY DEPLOYMENT

This section of SP 800-82 discusses the development and deployment of an industrial control system security program. In order to be successful, an organized defense in depth approach to security is required. It is also important to remember that security is not a one-time event, but a journey. Technology changes, operations change, and standards and regulations change, therefore the security needs of an industry facility change along with them.

The Instrumentation, Systems, and Automation (ISA) SP99 Committee [7] is developing a Manufacturing and Controls Systems Security Standard that addresses the development and deployment of an industrial control system security program is detail.

It is important to note that risk is a function of probability and consequence. Consequences of cyber attacks against an industrial control system can include:

- Reduction or loss of production at one site or multiple sites simultaneously
- Injury or death of employees
- Injury or death of persons in the community
- Damage to equipment
- Environmental damage
- Violation of regulatory requirements
- Product contamination
- Criminal or civil legal liabilities
- Loss of proprietary or confidential information
- Loss of brand image or customer confidence

It is also important to note that the risk model should support the business case. The objective is to reduce the risk to an acceptable level by mitigating the consequences from a successful attack, or by reducing the probability of attack by reducing the vulnerabilities that can be exploited by an attacker. Prioritization of vulnerabilities needs to be based upon cost and benefit. The objective is to provide the facility owner a business case for implementing at least the minimum set of control system security requirements to reduce the overall facility risk to an acceptable risk level.

Unfortunately, it would be very difficult to define a one-size-fits-all set of security requirements. A very high level of security may be achievable, but may be undesirable in many situations because of the loss of functionality and the cost that would be required to achieve this very high level of security. Security is a balance of risk versus cost and many situations will be different. In some situations the risk may be safety, health, or environmental related rather than purely an economic impact. The risk may have an unrecoverable consequence rather than a temporary financial setback.

A possible model is to develop recommended security requirements based on low, moderate and high levels of impact from potential consequences. This is also the model that is used in NIST SP 800-53 *Recommended Security Controls for Federal Information Systems* [8].

For industrial control systems, possible definitions for low, moderate and high levels [9] of security based on impact are:

Low

Product Controlled: Non hazardous materials or products, Non-ingested consumer products
Industry Examples: Plastic Injection Molding, Warehouse Applications
Security Concerns: Protecting people, Capital investment, Ensuring uptime

Moderate

Product Controlled: Some hazardous products and/or steps during production, High amount of proprietary information
Industry Examples: Automotive Metal Industries, Pulp & Paper, Semi-conductors
Security Concerns: Protecting people, trade secrets, capital investment, ensuring uptime

High

Product Controlled: Critical Infrastructure, Hazardous Materials, Ingested Products
Industry Examples: Utilities, PetroChemical, Food & Beverage, Pharmaceutical
Security Concerns: Protecting human life, Ensuring basic social services

RECOMMENED SECURITY CONTROLS (COUNTERMEASURES)

This section of SP 800-82 discusses recommended management, operational, and technical security controls (countermeasures) to mitigate the risk associated with the vulnerabilities.

MANAGEMENT CONTROLS

Management controls are the security controls (countermeasures) for an industrial control system that focus on the management of risk and the management of the industrial control system. The main management controls focus around the following areas:

- Risk Assessment
- Developing and implementing a security program
- System and services acquisition
- Security assessments

OPERATIONAL CONTROLS

Operational controls are the security controls (countermeasures) for an industrial control system that are primarily implemented and executed by personnel as opposed to the system. The main operational controls focus around the following areas:

- Personnel security
- Patch and configuration management
- Checklists
- Maintenance
- Network segmentation
- Incident response and disaster recovery plan
- Physical protection
- Media protection
- Awareness and training

TECHNICAL CONTROLS

Technical controls are the security controls (countermeasures) for an industrial control system that are primarily implemented and executed by the industrial control system through mechanisms contained in the hardware, software or firmware components of the system. The main technical controls focus around the following areas:

- User identification, authentication and authorization
- Data identification and authentication
- Device identification, authentication and authorization
- Logging and audit
- Secure communications
- Access control
- Intrusion detection and prevention
- Virus, worm and malicious code detection

GLOSSARY AND ACRONYMS

Appendix A and B of SP 800-82 provide a list of acronyms, and more importantly, a glossary of industrial control system security terms. An issue that exists within the industrial control systems environment (and others as well) is that common terminology needs to be well understood and accepted in order to fully address the security issues of these systems. It will be impossible to accurately address the security requirements of a “SCADA system” when there isn’t an accepted definition of what a “SCADA system” is. The glossary will attempt to harmonize definitions used within ISA SP99, AGA 12, IEC, ISO, NIST (FIPS and 800 series) and others. NIST is also investigating the idea of developing a “Top 10” mini-glossary, to potentially create a set of industry accepted definitions of the most used terms. NIST is seeking input on this idea.

CURRENT ACTIVITIES IN SCADA AND INDUSTRIAL CONTROL SYSTEM SECURITY

Appendix C of SP 800-82 provides a list and short description of current activities in SCADA/Industrial Control Security for reference. The list of activities includes:

- ISA SP99 (TR1, TR2, SP99 Standard)
- Process Control Security Requirements Forum (PCSRF)
- IEC TC 57 and 65
- DHS Process Control Systems Forum (PCSF)
- Institute for Information Infrastructure Protection (I3P) SCADA Initiative
- National SCADA Testbed
- NIST Industrial Control Systems Testbed
- Control Systems Security Center - INL
- Center for SCADA Security - SNL
- US-CERT Control Systems Center
- International Council on Large Electric Systems (CIGRE)
- IEEE Power Engineering Society (PES)
- North American Electric Reliability Council (NERC) CIP – formerly 1300
- Electric Power Research Institute (EPRI)
- Process Control Systems Cyber Security (PCSCS) Forum
- Chemical Industry Data eXchange (CIDX)
- American Petroleum Institute (API) 1164
- American Gas Association (AGA) 12
- ISO 17799 and 15408
- Applicable NIST SP 800 documents

SUMMARY

NIST has several ongoing efforts to address industrial control system security including the Process Control Security Requirements Forum (PCSRF) and Special Publication 800-82.

The PCSRF, formed in spring of 2001, is a 650-member working group of users, vendors, and integrators in the process control industry, which is addressing the cyber security requirements for industrial process control systems and components, SCADA and DCS systems, PLCs, RTUs and IEDs.

NIST Special Publication 800-82, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security*, scheduled for release in January 2006, provides guidance for establishing secure SCADA and industrial control systems. The document provides an industrial control system overview and typical system topologies to facilitate the understanding of the unique requirements for industrial control systems, identifies typical vulnerabilities and threats to these systems and provides recommended security countermeasures to mitigate the associated risks.

REFERENCES

[1] Process Control Security Requirements Forum (PCSRF), http://www.isd.mel.nist.gov/projects/processcontrol/

[2] National Information Assurance Partnership (NIAP), http://niap.nist.gov/pp/index.html

[3] PCSRF System Protection Profile for Industrial Control Systems (SPP-ICS), http://www.isd.mel.nist.gov/projects/processcontrol/SPP-ICSv1.0.doc

[4] Control Center PP, http://www.digitalbond.com/SCADA_security/Control_Center_PP.htm

[5] NIST Special Publications http://csrc.nist.gov/publications/nistpubs/

[6] *Common Vulnerabilities in Critical Infrastructure Control Systems*, Jason Stamp, John Dillinger, William Young, and Jennifer DePoy, Sandia National Laboratories report SAND2003-1772C, Albuquerque, New Mexico (2003).

[7] ISA-SP99, http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821

[8] NIST SP 800-53, *Recommended Security Controls for Federal Information Systems,* http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf

[9] Holly Beum, Interface Technologies, http://www.digitalbond.com/SCADA_Blog/2004_03_01_archive.html

DISCLAIMER

Commercial equipment and materials may be identified in order to adequately specify certain procedures. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.