www.iss.net

IBM Internet Security Systems White Paper

A Strategic Approach to Protecting SCADA and Process Control Systems

IBM Internet Security Systems
Ahead of the threat.™

Table of Contents

Abstract

This document provides an overview of the security weaknesses present in Supervisory Control and Data Acquisition (SCADA) and other Process Control Systems, the potential impact of those weaknesses and recommended steps for assessing and securing SCADA systems.

Overview

Process Control Systems (PCS) refer to the overall set of systems that remotely monitor and measure remote sensors from a centralized location. These sensors also typically possess some type of automated response capability when certain criteria are met.

A subset of PCS systems that manage systems over very large geographic areas are typically referred to as Supervisory Control and Data Acquisition systems or SCADA systems. SCADA systems make up the critical infrastructure associated with electric utilities, water and sewage treatment plants, and large-scale transportation systems like interstate rail.

Distributed Control Systems (DCS) and Industrial Control Systems (ICS) are also subsets of PCS systems. Both DCS and ICS systems are more geographically localized systems typically used in manufacturing plants and pharmaceutical production facilities.

Most SCADA and other PCS systems used by companies today were developed years ago, long before public and private networks or desktop computing were a common part of business operations. As a result, the need to incorporate security measures in these systems was not anticipated.

At the time, good security for SCADA systems meant limiting and securing the physical access to the network and the consoles that controlled the systems. Engineers rationalized that if the systems were suitably isolated from any physical entryways, and if access was limited to authorized personnel only, the systems were fully secure and unlikely to be compromised. This is no longer the case.

The increasingly networked and linked infrastructure of modern SCADA systems has rendered those early security plans obsolete. As companies have added new applications, remote access points and links to other control systems, they have introduced serious online risks and vulnerabilities that cannot be addressed by their physical control policies. Often, these risks are underestimated due to the complexity of the network architecture, the lack of formal network security guidelines and assumptions about the privacy of the network. Organizations are now realizing the security of these systems means more than physically separating the system and the components they control and monitor.

In fact, the online vulnerabilities in SCADA systems may pose as much risk for potentially significant failures in a power generation system as a physical attack.

PCS And SCADA Architectures

The basic structure of PCS systems is made up of a wide range of components and several different communication protocols. The operation of such a large and diverse infrastructure requires an extensive network of electronic devices, communications, and control and monitoring systems, such as:

- Field Devices
  - Remote Terminal Units (RTU)
  - Programmable Logic Controllers (PLC)
  - Intelligent Electronic Devices (IED)
  - Programmable Automation Controller (PAC)

- Management systems to monitor and control field equipment
  - Human Machine Interface (HMI)
  - SCADA Controller or Real Time Processor
  - Historian

- Communications
  - Ethernet, Wireless, Serial
  - Modbus, DNP3
  - ICCP, OCP

Network Architecture

Understanding the network architecture of PCS systems is critical to effectively evaluating their security posture. At the lowest level, the field devices are proprietary devices running embedded operating systems. These devices originally used serial communications to report to the centralized control center utilizing field bus protocols like Modbus and DNP3. Given the low bandwidth connections, these devices reported on a polling basis, or a report-by-exception basis to minimize network traffic. The SCADA controller is responsible for managing all of these communications, analyzing the data, and displaying the alerts and events on the HMI systems.

The Journey To Insecurity

Throughout the years, SCADA developers realized that they could gain enormous cost savings by utilizing standard operating systems instead of proprietary devices. Today's current PCS systems now use UNIX or Windows as the basis for all the systems in the control centers. These operating systems are even embedded within certain field devices today.

Additionally, developers realized that organizations could leverage the bandwidth provided on the larger data networks and, therefore, updated all of the field bus protocols to be encapsulated over standard TCP/IP protocols. The organizations then discovered that they could provide greater levels of service to their customers by integrating the control systems networks with their corporate networks, as all of the networks and protocols have become standardized.

Standardizing the PCS systems has now opened them to the same IT security challenges that have plagued other IT systems for years.

PCS Vulnerabilities

By conducting security assessments on a variety of PCS systems, IBM Internet Security Systems (ISS) consultants have identified some basic security issues impacting these devices. The following provides a high level overview of the critical security issues surrounding PCS systems:

- **Weak protocols leave systems vulnerable.** The underlying field bus protocols were never designed with security in mind. Most field devices are currently enabled with their own proprietary IP stack. These stacks were never tested outside of normal, SCAD.

  Testing shows that these devices are very prone to simple denial of service attacks and buffer overflows. Additionally, since field bus protocols were designed for serial communications, there is no built in authentication. This means the devices will accept connections from anyone, and legitimate packets will be processed without any additional user or system authentication.

- **Standard operating systems (Windows/Unix) leave the device open to well known security vulnerabilities.** Most PCS systems are not patched, or can not be patched as it will violate the vendor's service contract.

  Additionally, these systems are rarely hardened from a security perspective as it is feared the additional controls will impact the SCADA application, which can lead to serious exposures and risks.

- **PCS networks lack overall segmentation.** If firewalls are used, they are typically not well configured and only provide protection between the corporate network and the control center. Once the perimeter of the PCS network is breached, then the network is wide open. This also exposes the systems to standard worms, viruses and other malware.

- **PCS systems lack antivirus protection.** Many system vendors will not support antivirus applications. Plus, these systems are usually not accessing the Internet, making it difficult to download the daily virus updates that make antivirus technology legitimate.

- **Most IP-based communications within the PCS network rely on unencrypted communications.** This exposes the communications to eavesdropping and session hijacking.

- **Most PCS systems have limited-to-no logging enabled.** Logging is not enabled due to the focus on system reliability. However, if a security incident were to occur, it would most likely go completely unnoticed.

- **Many organizations still rely heavily on physical security measures.** Even with the amount of attention being paid to IT security, it is still rare to find security policies implemented in the organization. Many organizations have done little or no security awareness training with users, who collectively are one of the weakest links in a security program.

These are only a few of the potential risks associated with SCADA and Process Control Systems. IBM ISS recommends that organizations look for these weaknesses in any assessment of SCADA vulnerabilities and/or an organization's broader security posture.

Real Threats To SCADA Systems

Threats to SCADA networks are real and on the rise. Since 2000, there has been a tenfold increase in the number of successful cyber-attacks against SCADA systems at power generation, petroleum production, nuclear energy and water treatment facilities. At one Pennsylvania water treatment plant, a hacker exploited employee laptops, tunneling into the network through remote access applications. The hacker installed a virus and sypware and ultimately used the plant's computer system to distribute emails and pirated software. At Ohio's Davis-Besse nuclear power plant, the Slammer worm disabled a security monitoring system for nearly five hours. In another scenario, attackers, possibly from China, gained access to one of the computer networks that had hierarchical control over a number of PCS systems in California.

Threats to SCADA systems fall into two main categories: directed threats like industrial sabotage and coordinated terrorist attacks, and indirect threats like operational errors and viruses. The impacts of both types of threat remain serious. Potential outcomes include:

- Serious disruption to national critical infrastructure
- Loss of system availability
- Process interruption
- Equipment damage
- Asset mis-configuration
- Loss of data and confidentiality
- Personal injury
- Penalties resulting from regulatory violations
- Loss of customer and public trust

A number of regulatory agencies are now publishing security best practices for SCADA and PCS systems, but these are not requirements and don't have associated timelines, penalties or auditing practices identified.

Steps To Securing The SCADA Environment

A good approach to protect these critical systems is to leverage existing security best practices with SCADA priorities in mind. This requires the use of both administrative and technical controls and a defense-in-depth strategy that encompasses vulnerability assessment, threat prevention and policy. A defense-in-depth approach recognizes that the information security problem isn't just about IT. It involves people, process and technology.

The basic process is made up of four steps: establishing security, educating employees, enforcing policy and evaluating results.

Step One: Establish

The first step in any security program is to first establish where the security gaps exist within the existing business policy. In the case of SCADA systems, many vulnerabilities are inherent in the technology, but security must also account for the real-time processing and high availability SCADA requires. Internal and external assessments of network architecture, field and vendor networks, and applications will identify risks. A risk analysis must be conducted to prioritize the most critical areas first. Armed with this vulnerability and risk priority information, organizations can utilize policy to create a cultural change rather than a one-time security fix. Part of that policy change involves applying best practices like hardening the operating system (OS), disabling unnecessary ports and developing an appropriate patch process.

Network segmentation is another easy first step. Using demilitarized zones (DMZs), the IT department can isolate networks of different trust levels. This way, traffic from un-trusted networks never accesses the trusted network. Vendor access can be supported on a different DMZ and firewall logs can be used to watch for malicious traffic.

Applying intrusion prevention technology is also a strong component in establishing security. Intrusion prevention provides many advantages for internal segmentation. To ensure network availability, it fails open at the hardware layer, and offers real-time protection against viruses and worms. Preemptive intrusion prevention systems (IPS) can even protect vulnerabilities before a vendor-supplied patch is available, providing a window of time to test and apply patches. IPS can be used to block malicious traffic on multiple network segments. It provides real-time protection for remote access points, application-level protection for traffic that is allowed by the firewall and real-time alerting for additional levels of logging.

Step Two: Educate

End-users are the weakest link in security. To shore up this weak point, PCS network operators can team with third-party vendors to provide security awareness training for employees. The training reiterates the importance of security policy with end-users. In addition, educating IT staff about the importance of hardening the OS to ensure that vulnerabilities aren't reintroduced into the environment.

Step Three: Enforce

For enforcement, organizations can use automated scanning software to maintain system compliance. Working in coordination with SCADA engineers, this automated scanning performs heavier scans on less critical systems and leverages redundancy to ensure no system downtime. Recurring security assessments should also be part of enforcement and should encompass internal and external network segments and application and network layers. The results of these assessments should be used to constantly reevaluate risk reduction goals.

Step Four: Evaluate

In the evaluation phase, organizations should conduct security audits to ensure continued compliance with industry and government regulations. While many of these regulations are more like guidelines today, they will most likely become required for PCS operators moving forward. As part of the auditing process, organizations should measure the overall reduction in risk as a basis for calculating overall return on investment from security solutions.

Selecting the Right Security Provider

When selecting a security provider, several factors must be considered. Primary among them is SCADA system expertise. Security consultants should be Certified SCADA Security Architects with actual experience in the field working with these critical, real-time processing systems. In addition, it's helpful to work with a security provider that uses the SCADA Data Dictionary which can provide organizations with normalized data on threats targeting SCADA systems.

Lastly, organizations may want a security provider, known as a Managed Security Service Provider (MSSP) that can manage the day-to-day security tasks, allowing the internal IT staff to focus on more strategic projects. Using an outside MSSP to manage security can be done without compromising the trust of the SCADA network and can also correlate multiple security technologies, including firewalls, intrusion detection and intrusion prevention. Further, MSSPs offer 24/7/365 management and monitoring that would be cost prohibitive for most organizations.

SCADA Protection Solutions From IBM Internet Security Systems

Intrusion Prevention Systems

SCADA systems are vulnerable to a wide array of Internet threats attributable to the standard operating systems and network infrastructure upon which they rely, and to SCADA protocol-specific weaknesses. Working *Ahead of the threat*™, IBM Proventia® Network Intrusion Prevention Systems (IPS) block intrusion attempts, denial of service (DoS) attacks, malicious code, backdoors, worms and a growing list of new hybrid threats affecting SCADA systems.

Backed by IBM ISS X-Force® vulnerability-focused research, Proventia Network IPS features patented IBM Virtual Patch™ technology which provides out-of-the-box multi-layered protection for more than 1,000 high-risk and critical vulnerabilities or attacks by default. To minimize risk and maximize performance, suspicious traffic is analyzed using multiple traffic identification and analysis techniques, preventing the infection and unauthorized use of network resources. This preemptive protection is crucial for the security of mission-critical SCADA systems and important in supporting regulatory compliance and avoiding cleanup costs associated with security incidents.

Virtual Patch technology is a key feature of Proventia Network IPS. A Virtual Patch provides an impervious shield for newly discovered vulnerabilities until a vendor-developed patch can be tested and installed. This "mean time between vulnerability discovery and patching" can be translated into real ROI savings for Proventia appliances by reducing the time spent in testing and patching affected systems (estimated savings of 260 work days per year for a large enterprise).

Proventia Network IPS provides PCS and SCADA networks with several district advantages:

- As a Layer 2 device, the network will not require any IP readdressing

- As an inline security device, it includes hardware-level bypass allowing the device to fail open and preventing any network closures in the event of a hardware failure
- It's equipped with full SCADA protocol support for DNP3 and Modbus protocols with signatures for known protocol vulnerabilities.

SCADA Assessment Services

IBM ISS deploys a team of highly qualified security engineers to ensure a comprehensive approach to analyzing the vulnerabilities of PCS and SCADA systems. IBM ISS consultants include Certified SCADA Security Architects who have extensive experience conducting these assessments in the field. The IBM ISS Professional Security Services team will coordinate the SCADA and Process Control Systems Assessment closely with the client company to ensure an efficient use of resources and minimal impact on personnel.

IBM Internet Security Systems' assessment of a client's SCADA system entails a comprehensive information gathering approach that includes, but is not limited to:

- System assessment and evaluation
- Facilities reviews and personnel interviews
- Vendor information
- Functional evaluations and analysis of vulnerabilities.

Managed Security Services

IBM Managed Security Services offers customers comprehensive outsourced solutions for real-time security management including system monitoring, emergency response and 24/7/365 guaranteed* protection. The services go beyond simple event monitoring and device management, offering the industry's leading performance-based Service Level Agreements (SLAs) with a cash-back payment of up to $50,000. IBM ISS comprehensive Managed Security Services protect against the Internet's most critical threats, allowing organizations to minimize risk, control escalating security costs and demonstrate due diligence.

Summary

The complex architecture, interconnected nature and extreme sensitivity of SCADA and Process Control Systems mandate that organizations have a comprehensive plan for assessing and mitigating potential online vulnerabilities and threats. To do this successfully often requires the support of a security partner that not only has expertise in vulnerability assessment and planning, but that also has extensive experience working with SCADA and Process Control Systems.

IBM ISS is widely recognized as one of the industry's most skilled, effective and responsive group of security professionals. Just as important, the IBM ISS Professional Security Services team has been working closely with leading utility organizations to assess and implement SCADA-specific and utility-specific security policies and procedures. Through these engagements, IBM ISS has developed an expertise and process that has been tested and proven effective in SCADA and Control System environments.

** Money-back payment (for Managed Protection Services - Premium Level only): If IBM Internet Security Systems fails to meet the Security Incidents Prevention Guarantee shall be paid US$50,000 for each instance this guarantee has not been met. Please see IBM Internet Security Systems SLAs for more details.*

About IBM Internet Security Systems Professional Security Services

IBM ISS Professional Security Services deliver expert security consulting, helping organizations of all sizes reduce risk, achieve regulatory compliance, maintain business continuity and reach their security goals. IBM ISS Professional Security Services consultants are 100 percent security-focused and utilize proven consulting methods, based on ISO 17799 best security practices. Supported by the IBM ISS X-Force research and development team, IBM ISS Professional Security Services consultants are highly-skilled, senior security professionals. This team of security experts employs proprietary toolsets, the latest threat intelligence and advanced countermeasures to help build effective security programs that protect and enhance business operations.

About IBM Internet Security Systems

IBM Internet Security Systems (ISS) is the trusted security advisor to thousands of the world's leading businesses and governments, providing pre-emptive protection for networks, desktops and servers. An established leader in security since 1994, the IBM Proventia® integrated security platform is designed to automatically protect against both known and unknown threats, keeping networks up and running and shielding customers from online attacks before they impact business assets. IBM ISS products and services are based on the proactive security intelligence of its X-Force® research and development team – the unequivocal world authority in vulnerability and threat research. The IBM ISS product line is also complemented by comprehensive Managed Security Services and Professional Security Services. For more information, visit the IBM ISS Web site at www.iss.net or call 800-776-2362.

Learn More

For more information on how IBM Internet Security Systems has worked with PCS systems and organizations and its process for addressing SCADA and Process Control System vulnerabilities, please call 1-800-776-2362 or e-mail consulting@iss.net.

GLOBAL HEADQUARTERS

6303 Barfield Road
Atlanta, GA 30328
United States
Phone: (404) 236-2600
e-mail: sales@iss.net

REGIONAL HEADQUARTERS

Australia and New Zealand
Internet Security Systems Pty Ltd.
Level 6, 15 Astor Terrace
Spring Hill Queensland 4000
Australia
Phone: +61 (0)7 3838-1555
Fax: +61 (0)7 3832-4756
e-mail: aus-info@iss.net

Asia Pacific
Internet Security Systems K. K.
JR Tokyu Meguro Bldg. 3-1-1
Kami-Osaki, Shinagawa-ku
Tokyo 141-0021
Japan
Phone: +81 (3) 5740-4050
Fax: +81 (3) 5487-0711
e-mail: jp-sales@iss.net

Europe, Middle East and Africa
Ringlaan 39 bus 5
1853 Strombeek-Bever
Belgium
Phone: +32 (2) 479 67 97
Fax: +32 (2) 479 75 18
e-mail: isseur@iss.net

Latin America
6303 Barfield Road
Atlanta, GA 30328
United States
Phone: (404) 236-2709
Fax: (509) 756-5406
e-mail: isslatam@iss.net

Distribution: General
SM-SCADAWP-0107

IBM Internet Security Systems
Ahead of the threat.™