Securing Your Control System

Kim Fenrich
Manager, Project Solutions
Power Generation North America – Technology group
ABB Inc.
Wickliffe, Ohio, 44092

KEYWORDS

Control Systems, SCADA Systems, Security, Cyber Security, Open Systems, SCADA,

ABSTRACT

In the past, control systems used proprietary protocols, and were typically confined in an isolated, stand-alone environment. Today, because of the wealth of valuable information they contain, control systems are being connected to enterprise networks to allow business users access to real-time plant data. Since most modern control systems rely heavily on commercial operating systems and open standards such as Ethernet, TCP/IP, and web technologies that were originally developed for the business environment, this interconnectivity has introduced risks that did not exist in the past. This paper will provide an overview of the IT security issues in industrial control systems. General security concepts, objectives, best practices, and mitigation strategies will also be discussed.

INTRODUCTION

The control systems world is changing. Historically, process control systems — which include all industrial control, process control, supervisory control and data acquisition (SCADA), distributed control (DCS), and industrial automation systems (1) — were typically operated in an isolated or stand-alone environment, and did not share information or communicate with other systems. These systems were normally comprised of proprietary hardware, software, and protocols designed specifically to control and monitor sensitive processes. Since access to these control systems was greatly limited, and knowledge of these protocols was limited to a small population, control system network (also known as PCN's, or process control networks) security efforts were minimal, and focused primarily on physical measures.

Today, because of the vast amounts of valuable information they contain, and the need to make rapid, cost-driven decisions, stakeholders are demanding real-time plant information be readily available from any location. This has led many previously stand-alone control systems to become part of the "always connected" world, where real-time control system information can be easily accessed by business managers, engineers, and maintenance personnel, and vendors via corporate networks or Internet technologies. This increased connectivity, coupled with the adoption of standardized technologies, protocol implementations, and operating systems, has dramatically increased the focus on control system security.

UNDERSTANDING THE RISKS

Control systems can be vulnerable to a variety of types of cyber attacks that could have devastating consequences—such as endangering public health and safety; damaging the environment; or causing a loss of production, generation, or distribution by public utilities.

Because of this, numerous government agencies, standards bodies, industry organizations, and academic organizations have undertaken initiatives to increase the awareness of potential threats to control system users. The bulk of these programs, including *The National Strategy to Secure Cyberspace* (2) are intended to help establish security priorities, awareness and training programs, and threat and vulnerability reduction programs. The overwhelming message being presented by these organizations is that the number of externally initiated incidents is on the rise, and manufacturing facilities are almost certainly more connected, and vulnerable, than their owner\operators believe. While these programs have been successful in raising awareness on various levels, ranging from plant owners and operators to politicians; many statements being made by security vendors, consultants, and government agencies appear to be overly alarmist: "Many are beginning to believe the FUD about SCADA is merely the cyber-security industry employing scare tactics. This presentation will erase all doubt. Understanding SCADA security is easy: there is none. [. . .]" *(Abstract for talk by security vendor ISS at www.blackhat.com/html/bh-federal-06/bh-fed-06-speakers.html#maynor)* (3)

THE REALITY

Security incidents – which are defined as a violation of one or more security objectives – have and will continue to occur. While most organizations are reluctant to report security incidents for fear of embarrassment or financial repercussions, there have been a small number of well-documented incidents over the past few years. (4) (5) More recently:

> Confidential information, including incident response plans, were leaked out of a Japanese power plant through a virus infested computer with peer-to-peer file sharing applications in two independent incidents in the first half of 2006, following a similar incident in a different plant in 2005. (6)

As this evidence suggests, there is obviously some amount of risk faced by control systems. However, because there is little information sharing about actual attacks, and little conclusive statistical data available, the level of the risk is difficult to estimate.

THE THREATS

Security threats are defined as any circumstance or event with the potential to cause destruction, disclosure, modification of data, and/or denial of service, and come from both inside and outside of a facility.

Internal threats come from two main sources:

1.) Accidental incidents caused when an unknowledgeable, untrained, or careless employee performs an inadvertent action. Often, these incidents are abetted by complicated policies or procedures, improper authorization, or password sharing.
2.) Intentional incidents caused by disgruntled, dishonest, or unstable employees, contractors or guests with knowledge of the control system and authorized access.

External threats to control systems can be grouped as follows:

1.) Malware – Like any information system (IS), control systems are potentially vulnerable to viruses, worms, trojans and spyware. Although malware attacks are undirected – they don’t specifically attack control systems – they can impact the system by obstructing communications, corrupting data, installing back doors, and causing forced shutdowns.
2.) Hackers – Outsiders who are interested in probing, intruding or controlling a system for the challenge or notoriety.
3.) Terrorists – This threat distinguishes critical infrastructure systems from most IT systems, and the biggest source of concern for the US governments. According to the National Security Agency (NSA), foreign governments already have or are developing computer attack capabilities, and potential adversaries are developing a body of knowledge about U.S. systems and methods to attack these systems. (7)

THE CONSEQUENCES

While basically all computer systems are exposed to intrusion attempts, the potential consequences of such attempts are vastly different for different types of applications. For manufacturing and control systems – which can be connected directly to pipelines, electrical grids, and process equipment – a security incident can have severe consequences such as the endangerment of public safety, damage to the environment, loss of proprietary or confidential information, loss of production, damage to equipment, and loss of public confidence. This makes assessing the consequences of an industrial cyber attack more than simply a case of assigning a financial value. Although there are obvious direct financial impacts (i.e. loss of production or plant damage), other consequences such as the impact on a company's reputation can be far more significant than the cost of a production outage. Even minor regulatory violations can impact a company's reputation or license to operate. (8)

Due to the severity of these consequences, it's clear that efforts to protect control systems are necessary. However, even though technical advances for addressing control system security are being made regularly, no single solution or technology fits the needs of all organizations or applications.

Security Objectives

The primary objective of any security program is to protect the Confidentiality, Integrity, and Availability of the system. This model – known as the CIA Triad – is a widely used benchmark when evaluating the effectiveness of information systems security.

> *Confidentiality refers to the assurance of data privacy – Only the intended authorized people or devices –"the right people" – may access the data. Disclosure to unauthorized people or devices – "the wrong people" is a violation.*
>
> *Integrity refers to the assurance of data non-alteration – Data integrity is the certainty that the information has not been altered in transmission, from origin to reception*
>
> *Availability is the assurance that data and resources are obtainable at all times – Information should be available to people and devices who need it, when they need it.*

IT SECURITY IS DIFFERENT THAN CONTROL SYSTEM SECURITY

While modern control systems use many of the same technologies as IT systems and are beginning to resemble them, they also have many distinguishing characteristics. For instance, control systems have different performance and reliability requirements, require real-time response and have longer system lifecycles. Table 1 (9) provides a brief summary of the differences between IT and control systems.

TABLE 1. SUMMARY OF IT AND CONTROL SYSTEM DIFFERENCES

Category	Information Technology System	Industrial Control System
Performance Requirements	Non-real-time Response must be consistent High throughput is demanded High delay and jitter maybe acceptable	Real-time Response is time-critical Modest throughput is acceptable High delay and/or jitter is a serious concern
Availability Requirements	Responses such as rebooting are acceptable Availability deficiencies can often be tolerated, depending on the system's operational requirements	Responses such as rebooting may not be acceptable because of process availability requirements Outages must be planned and scheduled days/weeks in advance High availability requires exhaustive pre-deployment testing
Risk Management Requirements	Data confidentiality and integrity is paramount Fault tolerance is less important – momentary downtime is not a major risk Major risk impact is delay of business operations	Human safety is paramount, followed by protection of the process Fault tolerance is essential, even momentary downtime is not acceptable Major risk impact is regulatory non-compliance, loss of life, equipment, or production
Architecture Security Focus	Primary focus is protecting the IT assets, and the information stored on or transmitted among these assets. Central server may require more protection	Primary goal is to protect edge clients (e.g., field devices such as process controllers) Protection of central server is still important
Unintended Consequences	Security solutions are designed around typical IT systems	Security tools must be tested to ensure that they do not compromise normal ICS operation
Time-Critical Interaction	Less critical emergency interaction Tightly restricted access control can be implemented to the degree necessary	Response to human and other emergency interaction is critical Access to ICS should be strictly controlled, yet not hamper human-machine interaction
System Operation	Systems are designed for use with typical operating systems Upgrades are straightforward with the availability of automated deployment tools	Differing and custom operating systems often without security capabilities Software changes must be carefully made, usually by software vendors, because of the specialized control algorithms and perhaps modified hardware and software involved
Resource Constraints	Systems are specified with enough resources to support the addition of third-party applications such as security solutions	Systems are designed to support the intended industrial process, with minimal memory and computing resources to support the addition of security technology

Presented at the 50th Annual ISA POWID Symposium/17th ISA POWID/EPRI Controls & Instrumentation Conference; http://www.isa.org

Category	Information Technology System	Industrial Control System
Communications	Standard communications protocols Primarily wired networks with some localized wireless capabilities Typical IT networking practices	Many proprietary and standard communication protocols Several types of communications media used including dedicated wire and wireless (radio and satellite) Networks are complex and sometimes require the expertise of control engineers
Change Management	Software changes are applied in a timely fashion in the presence of good security policy and procedures. The procedures are often automated.	Software changes must be thoroughly tested and deployed incrementally throughout a system to ensure that the integrity of the control system is maintained. PCS outages often must be planned and scheduled days/weeks in advance
Managed Support	Allow for diversified support styles	Service support is usually via a single vendor
Component Lifetime	Lifetime on the order of 3-5 years	Lifetime on the order of 15-20 years
Access to Components	Components are usually local and easy to access	Components can be isolated, remote, and require extensive physical effort to gain access to them

While the primary security objectives are the same for each system, the CIA triad is reversed for control systems. Availability and fault tolerance are paramount – 99.99% uptime is required – because the process being controlled is continuous and can be unstable if not supervised; Integrity remains a necessity to ensure end-to-end data accuracy; and confidentiality – except for the protection of proprietary product recipes and plant security data – is of lower importance.

These differences pose multiple challenges. Many companies still assign the responsibility for control system security to the IT department, yet most IT departments are generally unfamiliar with the process reliability issues, performance requirements, and protocols of industrial equipment. This can result in the implementation of policies and procedures that simply don't work in the control system environment. In other companies, the IT and control system engineering staffs operate independently, with each performing similar functions. In this scenario, there is often little, or no, interaction between the two groups except when they meet at the plant network.

While it's clear that control and IT systems require different policies and procedures, IT staffs have far more experience with cyber security measures and what does and doesn't work. They understand open systems management, firewalls, and intrusion management. Controls systems staff should work closely with them, explain how the requirements differ, and then implement a strategy that makes sense.

THE COST OF SECURITY

Like everything else, however, security comes with a cost. While manufacturing facilities can't ignore the risks of security incidents, they also can't afford to employ infinite security measures. Having too much security can restrict access to information and data to those with authorization and create unnecessary cost; not enough security puts operating profits and people at risk. Since 100% security is not feasible, users should focus on critical areas and functions first, and apply security measures that are based on the value of the data or application. As a rule of thumb, plants should apply security measures that are proportional in cost to the value of data, risk, and probability associated with a security incident, and the potential consequences of the incident (10).

In some cases, the misapplication of technology results in significant overspending. Having skilled, properly trained personnel in place who follow defined practices and can carefully, effectively, and efficiently apply technology can help minimize overspending.

GENERAL SECURITY APPROACHES

Although there is no "silver bullet" for control systems, most can be adequately secured once the risks are understood. Establishing effective safeguards for control systems, the devices with which they interact, and the networks on which they reside require a multi-faceted, multi-level effort. That effort needs to focus not only on technology, but on people as well. This can be accomplished by focusing on two key principles. (11)

SECURITY IS A PROCESS, NOT A PRODUCT

The human factor is the weakest link in any activity. Security is no exception. Therefore, a key element in implementing and maintaining the security of a computer system is the establishment of effective IT security policies and procedures. While many of the same policies used for securing corporate IT systems can be applied, policies and procedures for control systems networks should also:

- Ensure control system security practices align with business and operational needs
- Define, document, and manage formal policy and standards for process control system security
- Establish training and awareness programs for control systems, IT, and 3rd party personnel
- Implement and enforce password policies for all personnel with access to the control system. These policies should be based on the principle of least privilege - every application, user, or subsystem should be restricted to the minimum number of rights necessary to fulfill its purpose.

- Include procedures for assessing and responding to security incidents and alerts, including how to respond to potential disasters
- Include plans for regular audits of control system network security (12)

To make the security policy effective, it must be practical and enforceable, and it must be possible to comply with the policy. The policy must not significantly impact productivity, be cost prohibitive, or lack support. This is best accomplished by providing clear organizational responsibility, and including both management and system administrator personnel in the policy development process. (13)

DEFENSE-IN-DEPTH

A fundamental principle that should be part of any network protection strategy is defense-in-depth. This good practice approach, also known as the 'onion approach', uses a security zone concept to secure both the network interior and exterior. The highest value target, typically the control system, is placed in the innermost zone where the greatest level of isolation and security measures are applied. (This approach is similar to protecting a castle using multiple walls that form concentric rings, with the castle at the center, one gate in each wall, and with security guards watching each gate.) See Figure 1.

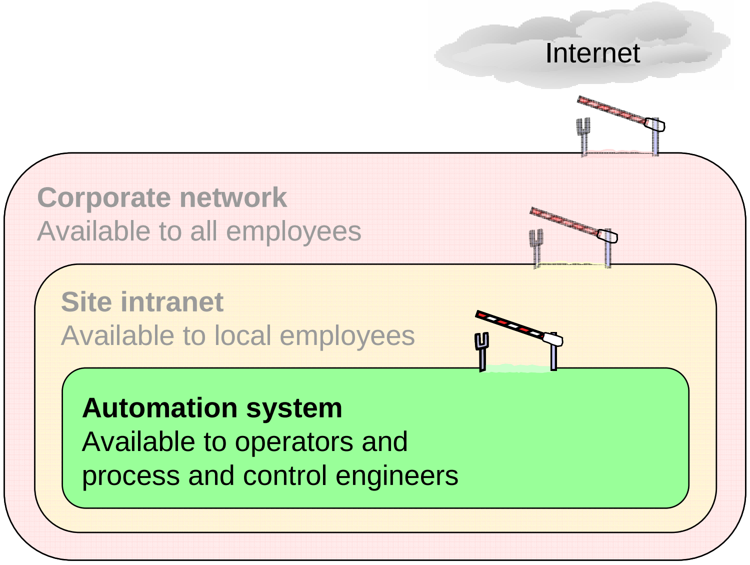
Internet
Corporate network
Available to all employees
Site intranet
Available to local employees
Automation system
Available to operators and
process and control engineers

FIGURE 1. SECURITY ZONE CONCEPT

The outer zones contain less valuable targets, and are protected by security mechanisms such as firewalls, gateways, and proxies – preferably different types for each zone – designed to detect and delay an attacker's movement inside and around each zone. These devices should be configured to pass only data that is absolutely essential for day to day operations.

GOOD PRACTICES

Over the past decade, numerous ‘good practices’ have been developed by IT departments, control system personnel, and industry organizations when deploying technical security measures or implementing procedural controls. These good practices, when implemented as part of a defense-in-depth strategy, can provide a solid foundation for an effective security program. Best practices for securing the network boundary and outer network zones, include:

- Securing remote and dialup connections with virtual private networks (VPN’s)
- Installation of firewalls and intrusion detection systems (IDS). Monitor and review their logs regularly
- Configure firewalls and routers to block all inbound network traffic except that which is explicitly required to maintain day to day operations.
- Regularly scanning all systems for viruses
- Adhering to defined security policies and procedures
- Deploying physical security measures to protect access by outsiders, or local unauthorized access.

High security zones, such as the control system network, should be small and independent, form their own domain, and follow the principle of least privilege. In addition, they should adhere to good practices such as, but not limited to:

- Prohibiting the use of Internet applications such as web-browsing, email, and messenger
- Hardening of all nodes in the system by disabling removable media, removing or disabling all unnecessary network connections, services, and file shares. Ensure that all remaining functions have appropriate security settings
- Installation of unauthorized software should be prohibited
- Connection of portable computers should be restricted. If they must be connected, they should be carefully scanned for malicious software before connection.
- The system should be isolated from other zones through properly configured, hardened firewalls
- All computers should be regularly scanned for viruses, and kept up to date with relevant, vendor recommended security updates.
- Physical access to all computers, network equipment, controllers, I/O systems, power supplies, should be restricted
- Security policies, procedures, and practices should be continuously reviewed and strictly enforced (14)

THE VENDORS ROLE

Despite the perception that all vendors are behind in addressing security within their control systems, some are making good progress. These vendors have acknowledged they have a responsibility to help users secure their systems, and have begun "baking" security features into new products while developing partnerships to help expand their expertise and scope of supply. This same group of vendors has implemented programs and services such as security patch testing, antivirus software accreditation, secure default settings, and security guidance and consulting. Solutions are now needed to help secure these vendors existing systems, and reduce the amount of time and effort required to maintain plant floor security.

Vendors who have remained neutral on their responsibilities and are not viewing security from a systems perspective must be forced to climb on board by users of their systems.

COLLABORATION IS KEY

Securing a control system is not only about technology; it's about people, relationships, processes and organizations. Only through effective collaboration between the IT department, control system engineers and system vendors can control systems be reliably secured. After all, who knows open systems management better than IT; and control systems better then the vendor. Since security is the ultimate responsibility of the system owner, it's important that users understand the risks, acknowledge the situation, and then implement a security program that meets the needs of the entire organization.

REFERENCES

(1) PA Consulting Group, "Good Practice Guide - Process Control and SCADA Security", PA Consulting Group and National Infrastructure Security Co-ordination Centre, London, England, Nov. 2006.

(2) "The National Strategy to Secure Cyberspace", United States Whitehouse, Washington, D.C., February, 2003.

(3) Naedele, Martin, "Addressing IT Security for Critical Control Systems", Proc. 40th Hawaii International Conference on Systems Science (HICSS-40 2007), Waikoloa Hawaii, January 3-6, 2007.

(4) Poulsen, Kevin, "Slammer worm crashed Ohio nuke plant network", www.securityfocus.com/news/6767, August, 2003.

(5) Spiegel, Rob, "Plant Security: Who's trying to Hack into Your Automation System", Automation World, September 2004, pp 38.

(6) Leyden, John, "Japanese power plant secrets leaked by virus," The Register, London, England, http://www.theregister.co.uk/2006/05/17/japan_power_ plant_ virus_ leak, May, 2006.

(7) United States Government General Accounting Office, "Critical Infrastructure Protection - Challenges and Efforts to Secure Control Systems", GAO-04-354, US General Accounting Office, Washington, D.C., March 2004.

(8) Byres, Eric and Lowe, Justin, "The Myths and Facts behind Cyber Security Risks for Industrial Control Systems," in Proc. of VDE Kongress, October, 2004.

(9) Stouffer, Keith, Falco, Joe and Kent, Karen, "Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security - Recommendations of the National Institute of Standards and Technology", SP800-82 Initial Public Draft, National Institute of Standards and Technology, Gaithersburg, MD., September, 2006

(10) Katzel, Jeanine, "Many Facets, One Point" Control Engineering, July, 2005.

(11) Naedele, Martin and Dzung, Dacfey, "Industrial Information System Security, Part 1", ABB Review, no. 2, pp. 66–70, 2005.

(12) Pauly, Thomas, "IS Security Considerations for Automation Systems" ABB Automation, Doc ID 3BSE032547A, February, 2005

(13) Idaho National Laboratory, "Control Systems Cyber Security: Defense in Depth Strategies", No. INL/EXT-06011478, U.S. Department of Homeland Security, May, 2006.

(14) Naedele, Martin and Vahldieck, Rolf, "Industrial Information System Security, Part 2", ABB Review, no. 3, pp. 74–78, 2005