ITL BULLETIN FOR AUGUST 2011

PROTECTING INDUSTRIAL CONTROL SYSTEMS – KEY COMPONENTS OF OUR NATION'S CRITICAL INFRASTRUCTURES

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Industrial control systems (ICS) are information systems that control industrial processes, such as manufacturing, product production, handling, and distribution. ICS are used in many industries: electric, water, oil and gas, chemical, pharmaceutical, pulp and paper, food and beverage industries; manufacture of automobiles, aerospace equipment, and other durable goods; and air and rail transportation.

These control systems are vitally important to the smooth operation of the nation's critical infrastructures, which are essential to the government and economy of the United States. Since critical infrastructures are often highly interconnected and mutually dependent systems, an incident in one infrastructure can affect other infrastructures, and cause operational failures. Approximately 90 percent of the nation's critical infrastructures are privately owned and operated, including the telecommunications, energy, financial services, manufacturing, water, transportation, healthcare, and emergency services sectors. Federal agencies also operate critical infrastructures including industrial processes, air traffic control, and mail handling.

In the past, industrial control systems could be operated relatively safely because they were usually physically isolated systems that used proprietary control protocols and implemented specialized hardware and software. Today, these systems are more likely to use information technology (IT) solutions that promote connectivity with corporate business systems and that support remote access capabilities. Standards-based computers, operating systems, and network protocols are replacing the earlier proprietary components. As a result, industrial control systems are beginning to be more like general information systems.

The integration of an organization's industrial control and business systems supports the use of new IT applications and capabilities. But this integration also increases the exposure of ICS to external threats, and increases the possibility of cyber security vulnerabilities and incidents. To address these threats and vulnerabilities, organizations may be able to apply security countermeasures that have been developed to address threats and vulnerabilities in traditional IT systems. In some cases, security solutions can be tailored to meet the special requirements of ICS environments; in other situations, new solutions may be needed to protect systems.

The Information Technology Laboratory (ITL) and the Engineering Laboratory (EL) at the National Institute of Standards and Technology (NIST) collaborated to develop a new guide to assist organizations that operate industrial control systems. NIST Special Publication (SP) 800-82, *Guide to Industrial Control Systems Security*, examines the vulnerabilities and threats to these systems and recommends a risk-based approach for establishing security countermeasures that will protect systems and meet an organization's specific business and operational requirements.

NIST Special Publication (SP) 800-82, *Guide to Industrial Control System (ICS) Security*

NIST SP 800-82 assists organizations in establishing and operating secure industrial control systems. Written by Keith Stouffer and Joe Falco of NIST, and by Karen Scarfone (formerly of NIST), the guide presents an overview of the different types of ICS, including: supervisory control and data acquisition (SCADA) systems; distributed control systems (DCS); and programmable logic controllers (PLC). The components, uses, and operations of these systems are discussed, along with the threats and vulnerabilities of the systems.

SP 800-82 summarizes the differences between ICS and IT systems. Threats to ICS are grouped by potential agents, and the vulnerabilities that result from policy and procedure, platform, network and communication weaknesses are analyzed. Security countermeasures to mitigate the associated risks are discussed. Detailed methods and techniques are identified for securing the various different types of ICS in accordance with varying levels of potential risk and impact on operations and individuals.

Other topics covered in the guide include how to develop a business case for establishing an ICS security program, and how to develop and implement a comprehensive security program to mitigate the risks. The guide discusses recommended practices for integrating security into network architectures typically found in ICS, and emphasizes the need for careful planning of any connections between the ICS and corporate networks.

The guide also features a discussion of the management, operational, and technical controls that have been developed to protect the confidentiality, integrity, and availability of information systems and information. The selection and assessment of appropriate security controls are important steps in the comprehensive process of managing risks and maintaining cost-effective security of information systems.

The appendices to SP 800-82 include a list of acronyms and abbreviations; a glossary of terms; an overview of the current activities being conducted by federal organizations, standards organizations, industry groups, and automation system vendors to recommend practices for ICS security; an overview of security capabilities and products that are available, and the research and development work that supports new products and technologies; an overview of the Federal Information Security Management Act (FISMA) implementation project, the supporting documents developed by NIST, and their applicability to protecting ICS; and a list of references.

NIST SP 800-82 is available here.

Types of Industrial Control Systems

Industrial control systems include the following types:

• **Supervisory control and data acquisition (SCADA) systems** are highly distributed systems used to control geographically dispersed assets, often scattered over thousands of square kilometers. Centralized data acquisition and control are critical to system operation. These systems are used in water distribution and wastewater collection systems, oil and natural gas pipelines, electrical power grids, and railway transportation systems. A SCADA control center performs centralized monitoring and control for field sites over long-distance communications networks, receiving information from remote station control devices (field devices) that control local operations such as opening and closing valves and breakers, collecting data from sensor systems, and monitoring the local environment for alarm conditions.

• **Distributed control systems (DCS)** are used to control industrial processes such as electric power generation, oil refineries, water and wastewater treatment, and chemical, food, and automotive production. DCS are integrated as a control architecture containing a supervisory level of control overseeing multiple, integrated subsystems that are responsible for controlling the details of a localized process. Feed back and feed forward control loops are used to achieve product and process control. DCS use PLC (see below) to accomplish the desired product and/or process tolerance around a specified set point.

• **Programmable logic controllers (PLC)** are computer-based solid-state devices that control industrial equipment and processes. While PLCs are control system components used throughout SCADA and DCS systems, they are often the primary components in smaller control system configurations used to provide operational control of discrete processes such as automobile assembly lines and power plant soot blower controls. PLCs are used extensively in almost all industrial processes.

Vulnerabilities and Risks to Industrial Control Systems

While similar in many ways to traditional information processing systems, industrial control systems are distinctive in their impact on the physical world. Failures and malfunctions pose significant risk to the health and safety of humans, serious damage to the environment, and financial impacts such as production losses, harm to the nation's economy, and compromise of proprietary information. ICS have unique performance and reliability requirements and often implement special operating systems and applications. When ICS are designed and operated, the goals of safety and efficiency for ICS may conflict with the goal of security.

The integration of ICS with IT networks decreases their physical isolation, and increases the need to secure ICS from remote, external threats. The increasing use of wireless networking puts ICS implementations at greater risk from adversaries who are in

relatively close physical proximity but who do not have direct physical access to the equipment. Threats to control systems can come from hostile governments, terrorist groups, disgruntled employees, malicious intruders, complexities, accidents, and natural disasters as well as malicious or accidental actions by insiders. The priority security objectives for ICS are protection of the availability, integrity, and confidentiality of systems and information.

Possible incidents that could impact ICS operations include:

• Blocked or delayed flow of information through ICS networks, which could disrupt ICS operation;

• Unauthorized changes to instructions, commands, or alarm thresholds, which could damage, disable, or shut down equipment, create environmental impacts, or endanger human life;

• Inaccurate information sent to system operators, either to disguise unauthorized changes, or to cause the operators to initiate inappropriate actions, resulting in negative effects;

• ICS software or configuration settings modified, or ICS software infected with malware, causing negative effects; and

• Interference with the operation of safety systems, and endangering human life.

Implementing Security Objectives

NIST recommends that organizations adopt the following security objectives when planning and developing ICS implementations:

• **Restrict logical access to the ICS network and network activity.** The system should use a demilitarized zone (DMZ) network architecture with firewalls to prevent network traffic from passing directly between the corporate and ICS networks, and should maintain separate authentication mechanisms and credentials for users of the corporate and ICS networks. The ICS should also use a network topology that has multiple layers, with the most critical communications occurring in the most secure and reliable layer.

• **Restrict physical access to the ICS network and devices.** Unauthorized physical access to components could cause serious disruption of the ICS's functionality. A combination of physical access controls should be used, such as locks, card readers, and/or guards.

• **Protect individual ICS components from exploitation.** Security patches should be deployed promptly after testing them under field conditions; all unused ports and services should be disabled; ICS user privileges should be restricted to those that are required for each person's role; audit trails should be tracked and monitored; and security controls

such as antivirus software and file integrity-checking software should be used where technically feasible to prevent, deter, detect, and mitigate malware.

• **Maintain functionality during adverse conditions.** The ICS should be designed so that each critical component has a redundant counterpart. Additionally, if a component fails, it should fail in a manner that does not generate unnecessary traffic on the ICS or other networks, or does not cause another problem elsewhere, such as a cascading event.

• **Restore system after an incident.** Incidents are inevitable and an incident response plan is essential. A major characteristic of a good security program is how quickly a system can be recovered after an incident has occurred.

To implement these security objectives, organizations should organize **a cross-functional cyber security team** composed of members who will share their knowledge and experience to evaluate and mitigate risk to the ICS. The cyber security team should include: a member of the organization's IT staff; control engineer; control system operator; network and system security expert; a member of the management staff; and a member of the physical security department. For continuity and completeness, the cyber security team should consult with the control system vendor and/or system integrator as well. The cyber security team should report directly to the organization's top management.

An effective cyber security program for an ICS should apply a **defense in depth** strategy that layers security mechanisms so that the impact of a failure in any one mechanism is minimized. A defense in depth strategy includes the following practices:

• Develop security policies, procedures, training, and educational material that apply specifically to the ICS.

• Consider ICS security policies and procedures based on Homeland Security alerts, deploying increasingly heightened security postures when threats are elevated.

• Address security throughout the life cycle of the ICS from system design to procurement to installation to maintenance to decommissioning of the system.

• Implement a network topology for the ICS that has multiple layers, with the most critical communications occurring in the most secure and reliable layer.

•Provide logical separation between the corporate and ICS networks using firewalls between the networks.

• Employ a DMZ network architecture to prevent direct traffic between the corporate and ICS networks.

• Ensure that critical components are redundant and are on redundant networks.

• Design critical systems for graceful degradation to prevent catastrophic cascading events.

• Disable unused ports and services on ICS devices after testing to assure that this action will not impact ICS operation.

• Restrict physical access to the ICS network and devices.

• Restrict ICS user privileges to those that are required by individuals to perform their jobs; for example, establish role-based access control and configure each role based on the principle of least privilege.

• Consider the use of separate authentication mechanisms and credentials for users of the ICS network and the corporate network.

• Use authentication technology, such as smart cards for Personal Identity Verification (PIV).

• Implement security controls such as intrusion detection software, antivirus software and file integrity-checking software, where technically feasible, to prevent, deter, detect, and mitigate the introduction, exposure, and propagation of malicious software to, within, and from the ICS.

• Apply security techniques such as encryption and/or cryptographic hash methods to ICS data storage and communications where appropriate.

• Deploy security patches after testing all patches under field conditions on a test system, and before installing on the ICS, if possible.

• Track and monitor audit trails on critical areas of the ICS.

Applying Security Controls

Security controls are the management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an informational system to protect the confidentiality, integrity, and availability of the system and its information. FISMA directs federal agencies to protect the information and information technology systems that support their operations and assets. FISMA emphasizes a risk-based policy for cost-effective security. To help federal agencies implement FISMA, NIST has developed standards and guidelines for protecting information systems and information based on assessments of risk. An important component of the risk assessment process is the selection and application of security controls

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations,* which was developed by the *Joint Task Force Transformation Initiative* Interagency Working Group with representatives from the Civil, Defense, and

Intelligence Communities, provides guidance in selecting and specifying security controls for information systems, and helps organizations use risk assessment methods in planning, developing, and maintaining cost-effective security. NIST SP 800-53 contains guidance on the selection of security controls for ICS.

NIST SP 800-82 supplements the guidance and information included in NIST SP 800-53 on the application of security controls and recommendations for ICS. NIST SP 800-82 also provides enhancements that may be required for some ICS, and guidance on the application of the enhancements. The supplemental guidance helps organizations determine whether a security control or enhancement may be applicable to their environments and whether tailoring may be needed.

Since the protection of ICS is a priority for protection of the nation's critical infrastructures, NIST started the Industrial Control System Security Project in cooperation with the ICS community in public and private sectors to develop specific guidance on the application of NIST documents to ICS. The project's participants have developed ICS cyber security case histories using actual ICS cyber security incidents. These case histories examine the ICS controls specified in NIST SP 800-53, determine whether they were implemented in the systems studied, and suggest what might have occurred if the controls had been implemented.

NIST plans to revise SP 800-53 in December 2011 with an update of current security controls, control enhancements, and supplemental guidance, as well as the tailoring and supplementation guidance, in the area of industrial control systems.

For More Information

For information about NIST standards and guidelines, and security-related publications, see here.

Information about NIST's information security programs is available from the Computer Security Resource Center here.