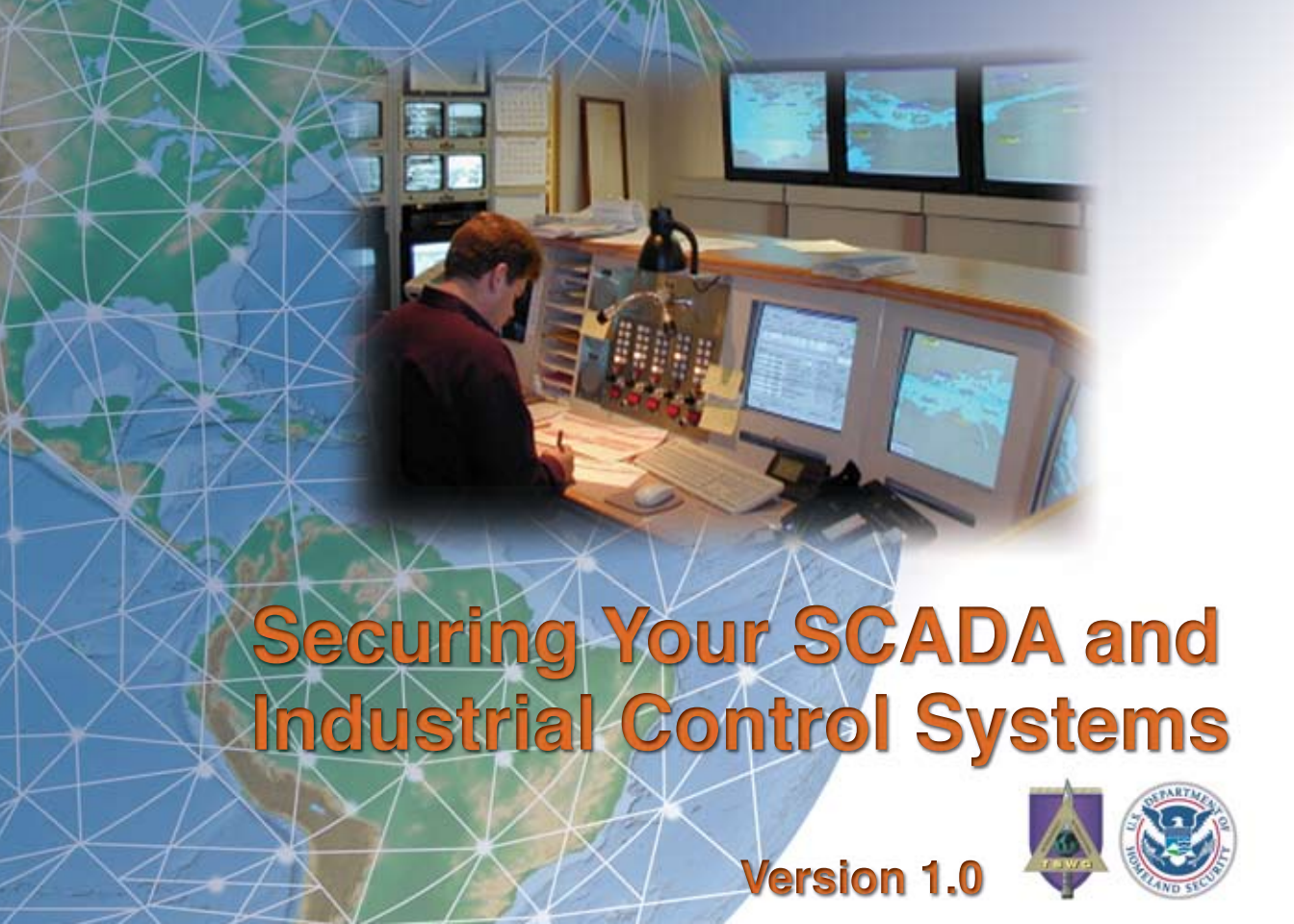


Securing Your SCADA and Industrial Control Systems

Version 1.0

Additional copies of this guide are available from the Government Printing Office. To order, cite stock number 008-022-00338-0, ISBN 0-16-075115-8. Orders may be placed via the Internet, phone, fax, and mail.

For secure ordering via the Internet, visit the U.S. Government Online Bookstore at http://bookstore.gpo.gov.

Phone: (202) 512-1800
Monday through Friday, 7:30 a.m.-5:00 p.m., eastern standard time

Fax: (202) 512-2250 at any time

Mail: send to:
Superintendent of Documents
P.O. Box 371954
Pittsburgh, PA 15250-7954

All orders require prepayment, either by check, money order, VISA, MasterCard, Discover/NOVUS, or GPO Deposit Account.

Disclaimer

The information in this guide is for informational purposes only and is not legal advice. The information is general and may or may not reflect the most current legal or technical developments. It does not constitute legal advice or substitute for obtaining legal advice from an attorney licensed in your state.

Unlimited release – Approved for public release.

Start Here

Purpose

This guidebook, developed by the Technical Support Working Group (TSWG), provides information for enhancing the security of Industrial Control Systems (ICS). The information is a comprehensive overview of industrial control system security, including administrative controls, architecture design, and security technology. This guide is intended for all sectors that use ICS technology. This is a guide for enhancing security, not a how-to manual for building an ICS, and its purpose is to teach ICS managers, administrators, operators, engineers, and other ICS staff what security concerns they should be taking into account.

Scope

This guide does not constitute a standard, and it is not a substitute for standards documents. Neither is this guide a comprehensive security manual. It does not go into detail about any specific technologies; it covers ICS security too broadly to be used as a standalone document. Standards and vendor documents should be consulted for help in properly securing a specific ICS configuration.

To Whom This Guide Applies

ICS is one term for a broader set of control systems, which include

- SCADA (Supervisory Control and Data Acquisition)
- DCS (Digital Control System)
- PCS (Process Control System)
- EMS (Energy Management System)
- AS (Automation System)
- Any other automated control system

Each industry has its own culture and set of terms. This guide is useful for any industry employing networked automation systems, regardless of the terms used.

Table of Contents

Table of Contents (cont.)

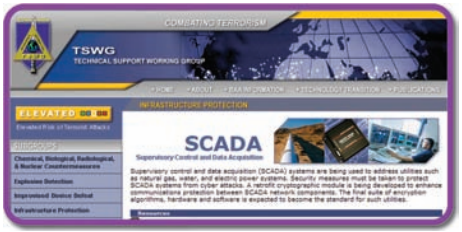
Table of Contents (cont.)

How to Use This Guidebook

This guide provides a foundation to help implement secure systems, secure existing systems, and make security a process rather than an afterthought. Working knowledge of ICS and basic cyber security is assumed.

Small colored boxes appear on the right-hand side of any page that implicitly refers to another section of the guide. Each such box contains the name of the section referred to and is that section's color.

The related TSWG website, http://www.tswg.gov/tswg/ip/scada.htm, contains more detailed information, updates, and job aids. Job aids include examples, templates, and references. A training support package will also be available with more detailed information for each section of the guide.



A Note on Anecdotes

Many sections in this guide begin with short anecdotes. These anecdotes provide examples of actual ICS security incidents, and are meant to demonstrate potential consequences of inadequate security practices. The anecdotes are in italic font with colored backgrounds for easy recognition.

Guidebook User Roles

This guide was written for a wide range of ICS staff. The roles defined below need not correlate perfectly with actual positions at a given ICS; they are meant to encapsulate job functions that must be performed by ICS staff in general. The icons appear at the beginning of each section, denoting the roles most applicable. All ICS staff, however, will benefit from reading each section.

ICS Engineer/Technician – Designs and maintains the ICS; participates in testing and designing security response guidelines (e.g. manual operations, incident response); maintains the system hardware.

ICS Operator – Maintains the day-to-day operations of the ICS; and administers users' accounts and applications.

ICS Security Administrator – Maintains security documentation; oversees the implementation of all security controls; evaluates and implements the results of security audits and assessments; investigates security incidents; and administers users' accounts and application security.

ICS Information Security Officer – Maintains all data contained in the system, and ensures that security controls are adequate for the protection of data.

ICS Manager – Approves all changes to the ICS, including exceptions to policy, purchases, new equipment, acquisitions, and ensures all security requirements are met.

Icons

The following icons are used throughout the guidebook to indicate other documents promoting the same recommendations, or cases where the TSWG website contains more detailed information.

See TSWG website for more information
http://www.tswg.gov/tswg/ip/scada.htm

See "21 Steps to Improve Cyber Security of SCADA Networks"
http://www.tswg.gov/tswg/ip/21_Steps_SCADA.pdf

See "NERC Critical Infrastructure Protection Standards CIP-002-1 through CIP-009-1"
http://www.nerc.com/~filez/standards-cyber.html
http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html

See "AGA-12: Cryptographic Protection of SCADA Communications General Recommendations"
http://www.gastechnology.org/webroot/downloads/en/1ResearchCap/1_1GasOps/AGASCADANews.pdf

See "NRC: Criteria for use of Computers in Safety Systems of Nuclear Power Plants"
http://www.nrc.gov/reading-rm/doc-collections/reg-guides/power-reactors/active/01-152/

See API's "Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries" and "Security Guidelines for the Petroleum Industry"
http://www.npra.org/publications/general/SVA_2nd_Edition.pdf

How to Use Frequently Requested Help

The Frequently Requested Help section lists common scenarios ICS engineers encounter that may require security knowledge and solutions. The list includes the page numbers of this guidebook that will assist the engineer in solving these problems with security in mind.

Not all issues can be covered by this guide. Every attempt has been made to cite the proper references where applicable.

Frequently Requested Help

Frequently Requested Help (cont.)

References

Section 1: Start Here

1. TSWG SCADA Security website
   http://www.tswg.gov/tswg/ip/scada.htm
2. "21 Steps to Improve Cyber Security of SCADA Networks"
   http://www.tswg.gov/tswg/ip/21_Steps_SCADA.pdf
3. NERC Critical Infrastructure Protection Standards CIP-002-1 through CIP-009-1
   http://www.nerc.com/~filez/standards-cyber.html
   http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html
4. "AGA-12: Cryptographic Protection of SCADA Communications General Recommendations"
   http://www.gastechnology.org/webroot/downloads/en/1ResearchCap/1_1GasOps/AGASCADANews.pdf
5. "NRC: Criteria for use of Computers in Safety Systems of Nuclear Power Plants"
   http://www.nrc.gov/reading-rm/doc-collections/reg-guides/power-reactors/active/01-152/
6. API's "Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries" and "Security Guidelines for the Petroleum Industry"
   http://www.npra.org/publications/general/SVA_2nd_Edition.pdf

Section 2: Setting the Foundation

1. HIPAA (Health Insurance Portability and Accountability Act of 1996)
   http://www.cms.hhs.gov/hipaa/
2. Gramm-Leach-Bliley Act
   http://www.ftc.gov/privacy/glbact/
3. Federal Information Security management Act (FISMA)
   http://csrc.nist.gov/sec-cert/
4. California Senate Bill 1386
   http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html
5. National Strategy to Secure CyberSpace
   http://www.whitehouse.gov/pcipb/
6. National Strategy for the Physical Protection of Critical Infrastructures and Key Assets
   http://www.whitehouse.gov/pcipb/physical.html
7. The Freedom of Information Act (FOIA)
   http://www.usdoj.gov/04foia/
8. Stamp, Campbell, Depoy, Dillinger, Young. "Sustainable Security for Infrastructure SCADA," SAND2003-4670C
   http://www.sandia.gov/scada/documents.htm
9. AMWA. Atkins, Cathy and Morandi, Larry. "Protecting Water System Security Information." September 2003. - Summarizes applicable legislation and lists FOIA exemptions
   http://www.amwa.net/security/NCSL_FOIA.pdf

Section 3: The Secure Design Process

1. Stamp and Berg. "A Reference Model for Control and Automation Systems in Electric Power," SAND 2005-1000C
   http://www.sandia.gov/scada/documents.htm
2. Campbell and Stamp. "A Classification Scheme for Risk Assessment Methods," SAND 2004-4233
   http://www.sandia.gov/scada/documents.htm
2. American Gas Association. AGA 12 - Cryptographic Protection of SCADA Communications General Recommendations. 2004
   http://www.gtiservices.org/security/AGA12Draft3r6.pdf
3. Government Classification
   http://en.wikipedia.org/wiki/Classified
4. Data Classification
   http://www.yourwindow.to/information-security/gl_dataclassification.htm

Section 4: Security Documentation

1. NIST 800-18 - Guide for Developing Security Plans for Information Technology Systems
   http://csrc.nist.gov/publications/nistpubs/
2. SANS System Security Plan
   http://www.sans.org/projects/systemsecurity.php
3. SANS Security Policy Project
   http://www.sans.org/resources/policies/

Section 5: Policy

1. Kilman and Stamp. "Framework for SCADA Security Policy," SAND 2005-1002C
   http://www.sandia.gov/scada/documents.htm
2. SANS Security Policy Project
   http://www.sans.org/resources/policies/
3. CobIT Control Objectives for Information and related Technology
   http://www.isaca.org/cobit.htm
4. BS7799
   http://www.thewindow.to/bs7799/
5. Anecdote
   http://www.computerworld.com/printthis/2004/0,4814,95615,00.htm

Section 6: Enforcement

1. API's "Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries" and "Security Guidelines for the Petroleum Industry"
   http://www.npra.org/publications/general/SVA_2nd_Edition.pdf
2. Sandia National Laboratories. SCADA Assessment Training Course
   http://www.sandia.gov/scada/training_courses.htm

Section 7: ICS Best Practices

1. American Gas Association. AGA 12 - Cryptographic Protection of SCADA Communications General Recommendations. 2004
   http://www.gtiservices.org/security/AGA12Draft3r6.pdf
2. National Institute of Standards and Technology FIPS PUB 140-2 "Security Requirements for Cryptographic Modules"
   http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
3. SANS SCORE
   http://www.sans.org/score/
4. SANS/FBI Top 20
   http://www.sans.org/top20/
5. NIST – National Institute of Standards and Technology
   http://csrc.nist.gov/publications/nistpubs/
6. CobIT Control Objectives for Information and related Technology
   http://www.isaca.org/cobit.htm
7. BS7799
   http://www.thewindow.to/bs7799/
8. NSA Guidelines
   http://nsa2.www.conxion.com/support/download.htm
9. Anecdote
   http://archives.openflows.org/electronetwork-l/msg00013.html

Section 8: Common Vulnerabilities

1. Stamp, Dillinger, Young, and Depoy. "Common Vulnerabilities in Critical Infrastructure Control Systems," SAND2003-1772C, May 2003
   http://www.sandia.gov/scada/documents.htm
2. Anecdote
   http://www.securityfocus.com/news/6767
3. FBI/SANS Top 20 Vulnerabilities
   http://www.sans.org/top20/

Section 9: Incident Handling and Response

1. NIST 800-61 Computer Security Incident Handling Guide
   http://csrc.nist.gov/publications/nistpubs/
2. DOE EIA
   http://www.nerc.com/~dawg/append-a.html
3. F-Secure Computer Virus Info Center
   http://www.f-secure.com/v-descs/
4. McAfee Virus Information Library
   http://vil.mcafee.com/
5. Sophos Virus Information
   http://www.sophos.com/virusinfo/
6. Symantec AntiVirus Research Center
   http://www.symantec.com/avcenter/

Section 9: Incident Handling and Response (cont.)

7. TrendMicro Virus Encyclopedia
   http://www.trendmicro.com/vinfo/virusencyclo/
8. Virus Bulletin VGrep Database
   http://www.virusbtn.com/resources/vgrep/
9. Vmyths Hoax
   http://www.vmyths.com/hoax.cfm
10. CIAC Hoaxbusters
    http://hoaxbusters.ciac.org/
11. DOE EIA
    http://www.nerc.com/~dawg/append-a.html
12. U.S. Department of Justice. Forensic Examination of Digital Evidence: A Guide for Law Enforcement:
    http://www.ncjrs.org/pdffiles1/nij/199408.pdf

Resources

Presidential Information

Homeland Security Presidential Directive on Critical Infrastructure: Identification, Prioritization, and Protection - HSPD-7 http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html
Executive Order 13231: Critical Infrastructure Protection http://www.fas.org/irp/offdocs/eo/eo-13231.htm
Presidential Decision Directive 63: Critical Infrastructure Protection http://www.fas.org/irp/offdocs/pdd-63.htm
The National Strategy to Secure Cyberspace http://www.whitehouse.gov/pcipb/
The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets http://www.whitehouse.gov/pcipb/physical.html

General Information

Cybersecurity for the Homeland DHS - December 2004 http://hsc.house.gov/files/cybersecurityreport12.06.04.pdf
Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors GAO - July 2004 http://www.gao.gov/cgi-bin/getrpt?GAO-04-780

General Standards

System Protection Profile for Industrial Control Systems NIST
http://www.isd.mel.nist.gov/projects/processcontrol/

IT Security for Industrial Control Systems NIST and PCSRF
http://www.isd.mel.nist.gov/documents/falco/ITSecurityProcess.pdf

General Guidance

21 Steps to Improve Cyber Security of SCADA Networks.
DOE and the President's Critical Infrastructure Protection Board
http://www.ea.doe.gov/pdfs/21stepsbooklet.pdf

Common Vulnerabilities in Critical Infrastructure Control Systems. Sandia National Laboratories
http://www.ea.doe.gov/pdfs/vulnerabilities.pdf

Sustainable Security for Infrastructure SCADA. Sandia National Laboratories
http://www.sandia.gov/scada/documents/SustainableSecurity.pdf

Applicable Laws

The Freedom of Information Act (FOIA)
http://www.usdoj.gov/04foia/

Control Frameworks

"CobiT Executive Summary," "CobiT Control Objectives," "CobiT Quickstart," http://www.isaca.org/cobit.htm
ISO-17799: Information Technology - Code of Practice for Information Security Management http://www.iso-17799.com/

Implementation Best Practices

Threat Alert System and Cyber Response Guidelines for the Electricity Sector NERC and CIPAG ftp://www.nerc.com/pub/sys/all_updl/cip/tas_cyber_v2.pdf
NERC CIPC Guides http://www.nerc.com/~filez/cipfiles.html
NERC Urgent Action Standard 1200-Cyber Security http://www.nerc.com/~filez/standards-cyber.html
NERC Urgent Action Standard 1300-Cyber Security http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html
FERC Security Standards for Electric Market Participants http://elibrary.ferc.gov/idmws/common/opennat.asp?fileID=9538944
ISA-SP99, Manufacturing and Control Systems Security http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821

Definitions

Access Control - Any method or technology used to control which hosts and/or users have access to a given resource.

Access Control List (ACL) - A table used by the computer system to identify access rights for each user to a particular system resource, such as a file directory, an individual file, or a device. In networking, the term refers to a list of the computing services available on a server, each with a list of hosts permitted to use the service.

Assets - Resources contributing to an organization achieving its mission. Assets may be tangible or intangible.

Authentication - The process of verifying the identity of a user or process attempting to access systems or resources.

Availability - The assurance that authorized users can access the information necessary to complete their jobs.

Bastion Host - A gateway between an inside network and an outside network designed to defend against attacks aimed at the inside network.

Classified - Data that is not to be released outside of the organization; release could result in harm to the organization (and could harm national security).

Company confidential - Private company information; release could damage the company.

Confidentiality - Protects information against unauthorized access or disclosure.

Definitions (cont.)

Configuration Management - Enforces the security plan and implementation guidance.

Cyber Security - The protection of information system assets and data by all means necessary, including physical protections.

DMZ (Demilitarized Zone) - Security enclaves, usually located logically between the inside and outside interface at a firewall, also called extranets.

Engineer/Technician - Designs and maintains the ICS, participates in testing and designing security response guidelines (manual operations, incident response), maintains the system hardware.

Event - An action or occurrence that can exploit a vulnerability.

Finger - Displays information about a user or users on a specified remote computer (typically a computer running UNIX).

For Official Use Only (FOUO) - Unclassified information exempt from public release and restricted to need-to-know access.

Implementation Guidance - A set of directives for the configuration, installation, and maintenance of specific technologies.

Definitions (cont.)

Information Security Officer - Responsible for all data contained in the system, responsible for ensuring that security controls are adequate for the protection of data.

In-Band - The technique of transmitting controlling information over the same LAN the information is controlling.

Integrity - Ensures the correctness and appropriateness of a piece of information content.

Intelligent Electronic Device (IED) - Consolidates data from field devices.

Link Encryption - Encrypts data as it is transmitted between two hosts in a network.

Manager - Responsible for approving all changes to the ICS, exceptions to policy, purchasing, and new equipment; ensures all security requirements are met.

Need-To-Know (NTK) - The business requirement that allows an individual to only have access to and knowledge of specific, protected information necessary to fulfill their work duties.

Operator - Maintains the day-to-day operations of the ICS.

Packet Encryption - Encrypts data between two applications running on different hosts.

Physical Security - The protection of assets using physical devices and entities (such as guns, gates, and guards), allowing access only to authorized individuals.

Definitions (cont.)

Principle of Least Privilege - A user or process is given no more privilege than necessary to perform a job.

Procedures - Document appropriate behavior for repeatable situations.

Programmable Logic Controller (PLC) - Devices that provide hardware interface for input sensors and output actuators.

Public - Data is not sensitive; release of this information poses no threat.

Reliability - Ensures that users can depend on the information and resources of a system to be accurate and available when needed.

Remote Access - Any access to a device that originates outside of the system's network.

Remote Access Server (RAS) - A server that is dedicated to handling users not on a LAN but needing remote access to it.

Remote Terminal Unit (RTU) - Data interface between a control station and remote control equipment and field devices.

Risk - The possibility that a particular threat will exploit a vulnerability resulting in a consequence of concern.

Definitions (cont.)

Risk Assessment - The determination of risks and risk levels acceptable by a system. This type of assessment must take into account expected adversaries and their capabilities, as well as the vulnerabilities of the system.

Security Administrator - Maintains security documentation; oversees the implementation of all security controls; evaluates and implements the results of security audits and assessments; investigates security incidents; and administers users' accounts and application security.

Security Enclave - An enclave is the container for data elements of like security characteristics. Security enclaves can be implemented as perimeters or as access controls on storage media or platforms.

Security Plan - Enumerates security guidelines for systems, or groups of systems, based on fundamental concepts from the security policy.

Security Policy - Translates the desired security and reliability control objectives for the overall business into enforceable staff directions and behaviors to ensure secure ICS design, implementation, and operation. Security Policy bridges the control framework to enforcement.

Single Point of Failure - Any component of a system that upon failure will cause a malfunction in the entire system.

Split Tunneling - The process of allowing a remote VPN user to access a public network (most commonly the Internet) at the same time that the user is allowed to access resources on the VPN.

Definitions (cont.)

Threat - A threat is a circumstance or event that can potentially cause harm to a system.

Virtual Private Network (VPN) - Any technology that allows confindential sharing of network resources across an insecure channel.

Vulnerability - A point of weakness in a system.

Vulnerability Assessment - The determination of possible security holes in a system. This type of assessment must take into account current technology and its possible uses and misuses.

Wipe (wiping software) - A method of removing data from electronic media. This method involves overwriting the existing data, usually multiple times.

Acronyms

ACL	Access Control List
AEPR	Alarm and Event Processing Routine
AES	Advanced Encryption Standard
AGC	Automatic Generation Control
AS	Automation Systems
AV	Antivirus
BOOTP	Bootstrap Protocol
CI	Critical Infrastructures
CM	Configuration Management
DCS	Digital Control Systems
DHS	Department of Homeland Security
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DoD	Department of Defense
EMS	Energy Management Systems
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act

Acronyms (cont.)

FOIA	Freedom of Information Act
FOUO	For Official Use Only
FTP	File Transfer Protocol
HIDS	Host-based Intrusion Detection Systems
HIPAA	Health Insurance Portability and Accountability Act
HMI	Human Machine Interface
HTTP	Hypertext Transfer Protocol (world wide web protocol)
I/O	Input/Output
ICCP	Inter-Control Center Communications Protocol
ICS	Industrial Control Systems
IDS	Intrusion Detection System
IED	Intelligent Electronic Device
IP	Internet Protocol
ISAC	Information Sharing and Analysis Center
ISO	Independent System Operators
IT	Information Technology
LAN	Local Area Network

Acronyms (cont.)

MAC	Media Access Control
MAN	Metropolitan Area Network
NERC	North American Electric Reliability Council
NIDS	Network-based Intrusion Detection System
NIST	National Institute of Standards and Technology
NTK	Need-To-Know
PCS	Process Control Systems
PCSRF	Process Control Security Requirements Forum
PLC	Programmable Logic Controller
PX	Power Exchange
RAS	Remote Access Services
RF	Radio Frequency
RFQ	Request for Quote
RTO	Regional Transmission Operator
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SMTP	Simple Mail Transfer Protocol (Internet email)

Acronyms (cont.)

SNMP	Simple Network Management Protocol
SPAN	Switch Port Analyzer
SSID	Service Set Identification (IEEE 802.11 wireless networks)
SSH	Secure Shell
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TSWG	Technical Support Working Group
UPS	Uninterruptible Power Supply
VPN	Virtual Private Network
WAN	Wide Area Network
WAP	Wide Area Protection

Standards and Association Links

Broad Based Links

- Instrumentation, Systems, and Automation Society
  http://www.isa.org/
- National Association of Regulatory Utility Commissioners
  http://www.naruc.org/
- Sandia National Labs Center for SCADA Security
  http://www.sandia.gov/scada/home.htm
- Process Control Systems Forum (PCSF)
  http://www.pcsforum.org/
- NIST Process Control Security Requirements Forum (PCSRF)
  http://www.isd.mel.nist.gov/projects/processcontrol/

Chemical Links

- Chemical Industry Data Exchange
  http://www.cidx.org/
- American Institute of Chemical Engineers
  http://www.aiche.org/

Standards and Association Links (cont.)

Electrical Links

- North American Electric Reliability Council (NERC)
  http://www.nerc.com/
- Electric Power Research Institute
  http://www.epri.com/
- Office of Energy Assurance
  http://www.ea.doe.gov/
- Electricity Sector Information Sharing and Analysis Center
  http://www.esisac.com/
- International Council on Large Electric Utilities
  http://www.cigre.org/ -or- http://www.cigre-usnc.org/
- National Council on Electricity Policy:
  http://www.ncouncil.org/

Energy Links

- Energy Information Sharing and Analysis Center
  http://www.energyisac.com/
- American Public Power Association
  http://www.appanet.org/
- National Association of State Energy Officials
  http://www.naseo.org/

Manufacture Links

- National Center for Manufacturing Sciences
  http://www.ncms.org/

Nuclear Links

- Nuclear Regulatory Commission
  http://www.nrc.gov/

Oil & Gas Standards Links

- Security Vulnerability Assessment Methodologies for the Petroleum and Petrochemical Industries API, May 2003
  http://api-ec.api.org/filelibrary/SVA_2003.pdf
- Security Guidelines for the Petroleum Industry - American Petroleum Institute
  http://api-ec.api.org/filelibrary/Security_Guidance2003.pdf

Standards and Association Links (cont.)

Oil and Gas Links

- Gas Technology Institute (GTI)
  http://www.gastechnology.org/
- American Gas Association
  http://www.aga.org/
- American Petroleum Institute
  http://api-ec.api.org/
- National Petroleum Council
  http://www.npc.org/
- National Petrochemical & Refiners Association
  http://www.npra.org/

Security Links

- Infragard
  http://www.infragard.net/
- Information System Security Association
  http://www.issa.org/
- Partnership for Critical Infrastructure Security
  http://www.pcis.org/
- Information Systems Audit and Control Association
  http://www.isaca.org/

Standards and Association Links (cont.)

Water Links

- Water Information Sharing and Analysis Center
  http://www.waterisac.org/
- Association of Metropolitan Water Agencies
  http://www.amwa.net/
- American Public Works Association
  http://www.apwa.net/
- Water Quality Association
  http://www.wqa.org/
- Water Environment Federation
  http://www.wef.org/
- National Rural Water Association
  http://www.nrwa.org/
- Association of State Drinking Water Administrators
  http://www.asdwa.org/
- Ground Water Protection Council
  http://www.gwpc.org/
- Association of Metropolitan Sewage Agencies
  http://www.amsa-cleanwater.org/
- American Water Works Association
  http://www.awwa.org/

ICS Primer

An ICS monitors and controls critical infrastructure equipment both locally and remotely. The system can be viewed as a collection of interconnecting devices and automated and human actions working together to monitor and control a particular infrastructure. The function and efficiency of an ICS depends on the types of equipment controlled and the communication methods employed by the ICS.

Local controls primarily protect equipment from damage by removing from service when set thresholds (temperature, pressure, current, etc.) are exceeded. Well-defined local control functions regulate and respond to system conditions within a specified range. Remote controls at control centers consolidate data from local equipment using automated and human actions.

Two Categories of ICS

Control systems can be broken into two broad categories: those deployed in a single location, such as those used in manufacturing or chemical plants, and those spread out over multiple locations, such as those used in electric power, oil and gas, or water systems.

Manufacturing and Chemical

In the manufacturing and chemical industries, ethernet or modem networks typically transmit control data between local equipment and several distributed control areas or centralized control areas. These industries refer to ICSs as Process Control Systems (PCSs) or Distributed Control Systems (DCSs) rather than as Supervisory Control and Data Acquisition (SCADA) systems. A typical system has an interconnected network of programmable logic controllers (PLCs) and control centers that communicate via local area network (LAN) fibers or wires, supplemented with gateways and modems or serial lines to carry out the monitoring and control functions of the field devices. Because Ethernet is high-speed and the serial devices are relatively close to the PLCs, monitoring and control of devices can be very rapid.

Electric Power, Oil and Gas, and Water

In the electric power, oil and gas, and water infrastructures, ICSs have one or a few centralized control stations to communicate with a multitude of remote stations, each with a Remote Terminal Unit (RTU) or PLC to concentrate data from the remote station devices. The remote station connections can be as simple as an RTU connected with direct hardwires to panels and field devices, or a more modern configuration with RTU connections to serial or Ethernet intelligent electronic devices (IEDs) (which consolidate data from the field devices). RTUs, PLCs, and individual IEDs can also be Internet Protocol (IP) addressable, allowing for direct monitor and control.

- SCADA – Supervisory Control and Data Acquisition (All-encompassing government term for automation systems)
- EMS – Energy Management System
- Protection – Relaying
- AGC – Automatic Generation Control
- WAP – Wide Area Protection
- DMS – Distribution Management System

Related Works in Progress

We refer readers to the future publication of NIST 800-82 – "Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security" to be released as a public draft in September 2005 and as a final publication in January 2006. This publication may be found on the Internet at:

- NIST Special Publications: Computer Security Resource Center - CSD
  http://csrc.nist.gov/publications/nistpubs/

Additional resources that will be valuable for SCADA security may be found on the Internet at:

- NIST Process Control Security Requirements Forum (PCSRF)
  http://www.isd.mel.nist.gov/projects/processcontrol/

- Institute for Information Infrastructure Protection (The I3P)
  http://www.thei3p.org/

TSWG Mission: Conduct the National Interagency Research and Development program for Combating Terrorism through rapid research, development and prototyping.

Please contact TSWG at ipsubgroup@TSWG.gov to provide comments or suggestions on this publication or to request further information on the TSWG and it's programs.