

Securing Industrial Control Systems

A guide for properly securing Industrial Control Systems operating in a Microsoft Windows environment.

Revision 1.4

Last Revision: 4/12/2007

**Wonderware
Invensys Systems, Inc.**

AGREEMENT TO TERMS OF USE OF THE DOCUMENT.

These Terms of Use (the "Terms of Use") apply to "Securing Industrial Control Systems." (The Document)

Permission to use The Document is granted, provided that (1) the copyright notice below appears in all copies and that both the copyright notice and this permission notice appear, (2) use of information from The Document is for informational use only and will not be copied or posted on any network computer or broadcast in any media without the prior, express written permission of Invensys and (3) no modifications of The Document is made. Use for any other purpose is expressly prohibited by law, and may result in severe civil and criminal penalties. Violators will be prosecuted to the maximum extent possible.

INVENSYS AND/OR ITS RESPECTIVE SUPPLIERS MAKE NO REPRESENTATIONS ABOUT THE SUITABILITY OF THE INFORMATION CONTAINED IN THE DOCUMENT AND RELATED GRAPHICS PUBLISHED IN THE DOCUMENT FOR ANY PURPOSE. ALL SUCH INFORMATION AND RELATED GRAPHICS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. INVENSYS AND/OR ITS RESPECTIVE SUPPLIERS HEREBY DISCLAIM ALL WARRANTIES AND CONDITIONS WITH REGARD TO THIS INFORMATION, INCLUDING ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT.

LIABILITY LIMITATIONS OF THE DOCUMENT

IN NO EVENT SHALL INVENSYS AND/OR ITS EMPLOYEES, AGENTS OR RESPECTIVE SUPPLIERS BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THE DOCUMENT, OR PROVISIONS OF OR FAILURE TO PROVIDE SERVICES. THE INFORMATION AND RELATED GRAPHICS PUBLISHED IN THE DOCUMENT MAY INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY MADE TO THE INFORMATION HEREIN. INVENSYS AND/OR ITS RESPECTIVE SUPPLIERS MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED HEREIN AT ANY TIME, WITHOUT NOTICE.

USE OF SERVICES.

Some information in The Document may contain links to (URLs) informational pages, chat areas, news groups, forums, communities, calendars, photo albums and/or other message or communication facilities designed to enable you to communicate with others (each a "Communication Service" and collectively "Communication Services"). You agree to use the URLs contained within The Document according to the provisions of the owners of the websites. INVENSYS IS NOT RESPONSIBLE FOR THE 3rd PARTY URLs OR THE CONTENT ON THEM. By way of example, and not as a limitation, you agree that when using the links, you will not:

upload, post, email, transmit or otherwise make available any Content that is unlawful, harmful, threatening, abusive, harassing, tortious, defamatory, vulgar, obscene, libelous, invasive of another's privacy, hateful, or racially, ethnically or otherwise objectionable;

harm minors in any way;

impersonate any person or entity, including, but not limited to, a Invensys official, forum leader, guide or host, or falsely state or otherwise misrepresent your affiliation with a person or entity;

forge headers or otherwise manipulate identifiers in order to disguise the origin of any Content transmitted through the Service;

upload, post, email, transmit or otherwise make available any Content that you do not have a right to make available under any law or under contractual or fiduciary relationships (such as inside information, proprietary and confidential information learned or disclosed as part of employment relationships or under nondisclosure agreements);

upload, post, email, transmit or otherwise make available any Content that infringes any patent, trademark, trade secret, copyright or other proprietary rights ("Rights") of any party;

upload, post, transmit or otherwise make available any unsolicited or unauthorized advertising, promotional materials, "junk mail," "spam," "chain letters," "pyramid schemes," or any other form of solicitation, except in those areas (such as shopping rooms) that are designated for such purpose;

upload, post, email, transmit or otherwise make available any material that contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment;

disrupt the normal flow of dialogue, cause a screen to "scroll" faster than other users of the Service are able to type, or otherwise act in a manner that negatively affects other users' ability to engage in real time exchanges;

interfere with or disrupt the Service or servers or networks connected to the Service, or disobey any requirements, procedures, policies or regulations of networks connected to the Service;

intentionally or unintentionally violate any applicable local, state, national or international law, including, but not limited to, regulations promulgated by the U.S. Securities and Exchange Commission, any rules of any national or other securities exchange, including, without limitation, the New York Stock Exchange, the American Stock Exchange or the NASDAQ, and any regulations having the force of law;

"stalk" or otherwise harass another; or

collect or store personal data about other users.

Invensys has no obligation to monitor the URLs provided within The Document. However, Invensys reserves the right to review materials posted at the URLs and to remove any web links in its sole discretion.

Always use caution when giving out any personally identifiable information about yourself or your children in any Communication Services. Invensys does not control or endorse the content, messages, or information found in any Communication Services and, therefore, Invensys specifically disclaims any liability with regard to the Communication Services and any actions resulting from your participation in any Communication Services. Managers and hosts are not authorized Invensys spokespersons, and their views do not necessarily reflect those of Invensys.

Materials uploaded to the Communication Services may be subject to posted limitations on usage, reproduction, and/or dissemination; you are responsible for adhering to such limitations if you download the materials.

LIMITATIONS ON WORLDWIDE USE.

The Document is presented by the Invensys from within the United States, and Invensys makes no representation that materials in The Document are appropriate or available for use in locations outside the United States. Although The Document is accessible worldwide, not all features, products or services discussed, referenced, provided or offered through or within The Document are available to all persons or in all geographic locations, or appropriate or available for use outside the United States. Invensys reserves the right to limit, in its sole discretion, the provisions and quantity of any feature, product or service to any person or geographic area. Any offer for any feature, product or service made on this Website is void where prohibited. If you choose to access The Document from outside the United States, you do so on your own initiative and you are solely responsible for complying with local laws.

Neither The Document, nor any underlying information or technology may be downloaded or otherwise exported or re-exported into, or to a national or resident of, any country to which the United States has embargoed goods (for example, Cuba, Iraq, Libya, North Korea, Sudan, Syria) or to anyone on the U.S. Treasury Department's list of Specially Designated Nations or the U.S. Commerce Department's Table of Denial Orders. By downloading or using any element of The Document, you are agreeing to the foregoing and you are certifying that you are not located in, under the control of, or a national or resident of any such country or on any such list. In addition, you are responsible for complying with any and all local laws in your jurisdiction which may impact your right to use the Website.

GOVERNING LAW; DISPUTE RESOLUTION.

You agree that all matters relating to your access to or use of The Document, including all disputes, will be governed by the laws of the United States and by the laws of the State of California without regard to its conflicts of laws provisions. You agree to the personal jurisdiction by and venue in the state and federal courts in Orange County, California, and waive any objection to such jurisdiction or venue. Any claim under these Terms of Use must be brought within one (1) year after the cause of action arises, or such claim or cause of action is barred. No recovery may be sought or received for damages other than out-of-pocket expenses, except that the prevailing party will be entitled to costs and attorneys' fees. In the event of any controversy or dispute between Invensys and you arising out of or in connection with your use of the Website, the parties shall attempt, promptly and in good faith, to resolve any such dispute. If we are unable to resolve any such dispute within a reasonable time (not to exceed thirty (30) days), then either party may submit such controversy or dispute to mediation. If the dispute cannot be resolved through mediation, then the parties shall be free to pursue any right or remedy available to them under applicable law.

LINKS TO THIRD PARTY SITES.

SOME LINKS IN THE DOCUMENT WILL LET YOU LEAVE INVENSYS' WEBSITES. THE LINKED SITES ARE NOT UNDER THE CONTROL OF INVENSYS AND INVENSYS IS NOT RESPONSIBLE FOR THE CONTENTS OF ANY LINKED SITE OR ANY LINK CONTAINED IN A LINKED SITE, OR ANY CHANGES OR UPDATES TO SUCH SITES. INVENSYS IS NOT RESPONSIBLE FOR WEBCASTING OR ANY OTHER FORM OF TRANSMISSION RECEIVED FROM ANY LINKED SITE. INVENSYS IS PROVIDING THESE LINKS TO YOU ONLY AS A CONVENIENCE, AND THE INCLUSION OF ANY LINK DOES NOT IMPLY ENDORSEMENT BY INVENSYS OF THE SITE.

COPYRIGHT NOTICE.

Copyright © 1997-2007 Invensys Systems, Inc., 26561 Rancho Parkway South, Lake Forest, CA 92630 U.S.A.

All rights reserved. No part of this documentation shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Invensys Systems, Inc. No copyright or patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this documentation, the publisher and the author assume no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information contained herein.

The information in this documentation is subject to change without notice and does not represent a commitment on the part of Invensys Systems, Inc. The software described in this documentation is furnished under a license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of these agreements.

Portions of this document have been based upon or excerpted from ANSI/ISA-95.00.01-2000, Enterprise-Control System Integration Part 1: Models and Terminology, and ANSI/ISA-95.00.02-2001, Enterprise-Control System Integration Part 2: Object Model Attributes. Copyright ISA 2000 and 2001. Reprinted by permission. All rights reserved.

Invensys; Wonderware; ActiveFactory; ArchestrA; DT Analyst; FactorySuite; FactorySuite A2; InBatch; InControl; IndustrialSQL Server; InTouch; Manufacturing Execution Module; QI Analyst; SCADAAlarm; SuiteLink; SuiteVoyager; WindowMaker; WindowViewer; WonderWorld; Every system in your plant, working in concert; the Visualize, Analyze, Optimize symbols; SPCPro and Visualize, Analyze, Optimize are trademarks or service marks of Invensys plc, its subsidiaries and affiliated companies. All other brands and product or service names may be the trademarks or service marks of their respective owners.

Invensys Systems, Inc.
26561 Rancho Parkway South
Lake Forest, CA 92630
1.949.727.3200
<http://www.wonderware.com>

Contents

Foreword to the First Release.....15

Before You Begin18

About This Document	18
Audience.....	18
Assumptions	18
Document Conventions	19
Where to Find Additional Information.....	19
Wonderware Security Central Website	19
ArchestrA Community Website.....	19
Technical Support	20

CHAPTER 1: Industrial Control Systems Review.....21

SCADA and DCS Review.....	22
ICS Operation Review	23
Key ICS Components	24
SCADA System Review.....	26
Distributed Control Systems Review	30
SCADA and DCS Examples by Industry	32
ICS System Review Summary	33

CHAPTER 2: Defining ICS Security Risk Areas.....35

ICS and IT System Risk Overview	36
ICS and IT System Risk Comparison and Analysis	36
Requirements Comparison Summary	39
Assessing Security Risks	40
Standardized Protocols and Technologies	40
Increased Connectivity	40
Insecure and Rogue Connections	41
Public Information	42
Potential ICS Vulnerabilities	42
Assessing ICS Vulnerabilities	43
Policies and Procedures	43
Platform Security Vulnerabilities	48
Infrastructure Assessment.....	54
Detailed Network Component Considerations	60
Software.....	62
Other Manufacturing Systems Components.....	64
Security Threats and Attack Scenarios.....	65

ICS Attack Scenarios.....	67
Attack Event Documentation	68
Attack Event Categories and Descriptions	70
Detecting and Preventing Insider Threats	72
Best Practices for Stopping Insider Attacks	73
Case Studies.....	76

CHAPTER 3: Developing the ICS Security Program97

Developing the ICS Security Business Case.....	98
Defining ICS Security Benefits	98
Defining Potential Impacts and Consequences	99
Key Business Case Components	100
Building the Business Case	100
Presenting the Business Case to Leadership	101
Developing a Comprehensive Security Program.....	102
Building a Cross-Functional Team.....	102
Defining Charter and Scope	103
Defining Policies and Procedures.....	103
Defining ICS Assets	104
Performing the Vulnerability Assessment.....	104
Defining the Mitigation Controls	107
Providing Training and Security Awareness	107
Managing Risk	108
Creating ICS Security Controls.....	112
Management Controls	113
Operational Controls	118
Technical Controls.....	132
Controlling Access	138
System and Communications Protection.....	142

CHAPTER 4: Managing Security Patches and Virus Protection..... 147

Managing Security Patches	148
Setup	148
Change Initiation	149
Security Patch Release	150
Virus and Malware Protection.....	151
Summary	155
Technical References.....	155

CHAPTER 5: ICS Security Recommendations .. 157

Security Perspective	158
----------------------------	-----

Product Security Statement.....	158
Defining Computer Interactions	158
Third Party Applications in the Control Environment	160
Altering IT Strategies	160
Defining the ICS Security Environment.....	162
Defining the Single Endpoint Device	163
Summary Security Recommendations.....	164
Control System Industry LAN Security Recommendations	166
Implementing Network Firewalls	167
Deploying Firewalls in the ICS	168
Using Firewalls to Separate the Control Network.....	170
Segmenting the Process Control and Enterprise Networks	170
Summary Firewall Policies for ICSs	173
Recommended Firewall Rules for Specific Services	176
Specific ICS Firewall Issues.....	179
Control System Industry SCADA Security Recommendation	182
Defining the Secure Process Control Environment.....	183
Defining the Layered Security Model	183
The OSI Model and Securing a Control System	185
Transport Driver Interface	186
Security Changes Above the TDI Line.....	186
Security Changes Below the TDI Line.....	187
Using IPsec to Secure Control Systems	188
IPsec in the Business System Environment.....	188
IPsec in the Control System Environment.....	188
Configuring IPsec in the Single Endpoint Device	190
IPsec Configuration Notes	191
Defining the ICS Security Layers	194
Alternatives to VPN Tunnels for Unsecurable Devices	194
Introduction	194
Defining and Establishing Level 1 Security.....	195
Level 1 Security: Establish the IPsec Security Perimeter.....	195
Level 1 Security Variations.....	201
Level 2 Security: Machine-Level Firewalls	205
Level 3 Security: Secure Routing	206
Level 4 Security: Secure Perimeter Gateway Devices	206

CHAPTER 6: Configuring IPsec and Domain Isolation for the ICS Environment209

Configuration example of the IPsec perimeter for ICS	210
Creating the Organizational Unit.....	210
Configuration example of the Organizational Unit (OU) for Machine Communication	211
Configuring IPsec Transport Mode.....	211
Configuration example of Unsecured Device Communication	223
Monitoring the VPN Device	232
IPsec Configuration Summary	241

APPENDIX A: References for more help and information243

 Organizations:244

 Microsoft Domain Isolation:244

 Articles and Books:245

 Useful RSS Feeds.....245

 Additional Links245

Index251

Foreword to the First Release

Wonderware is proud to offer you the first release of Securing Industrial Control Systems. This document is an ambitious work and represents the current leading edge in Automation and Process Control Security Guidance. It has been more than a year in the making and has included hundreds of lab and research hours, and direct contributions from, and long technical conversations with a number of principle individuals both inside and outside the company.

Additionally, there are many contributions from industry organizations and standards bodies including:

ISA (The Instrumentation, Automation and Systems Society)

NERC (North American Reliability Council)

AGA (American Gas Association)

API (American Petroleum Institute)

IEC (International Engineering Consortium)

IEEE (Institute of Electrical and Electronics Engineers, Inc.)

ISO (International Organization for Standardization)

NIST (National Institute of Standards and Technology) who is speaking for the DHS (Department of Homeland Security) in regard to Automation and Control in government regulated industries.

During the past year (2006) there has been a great condensation of ICS security knowledge and information from standards bodies and experts from all over the world that has come to focus in many conferences, discussions, and focus groups. The information contained within this manual represents Best Practice resulting from this industry guidance.

Regardless of how much information is here or what technologies and security techniques are discussed, it is important to remember that there is no "magic bullet" for security. No "black box" can be purchased, no advanced operating system can be installed, no software or hardware can be utilized that will immediately end all of your security issues and concerns. The requirement for ongoing pro-active security is here to stay for any critical enterprise.

This manual discusses the aspects of securing Windows-based business network designs and compares them to Windows-based Control Systems (herein called ICS or Industrial Control Systems) and the legacy or unsecurable IP-based equipment that is generally attached to them. This equipment is the "Achilles heel," or most vulnerable aspect of the system, when trying to secure it. These unsecurable devices have been largely ignored in the past, usually because of the belief that since they do not run a Windows OS, then they are not any kind of serious threat.

The past practice has been to rely on each individual manufacturer to attempt to secure their particular application or device. This process methodology has further segregated and divided any otherwise secure ICS or SCADA System into pieces that are virtually impossible to examine holistically for any type of all-encompassing security, until finally when a breach happens somewhere in the system. This situation leaves most IT departments feeling unsure about what is and is not secure within their domains.

Creating a comparison between the differing network types has become necessary throughout all industry security guidance because ICSs have been traditionally secured using common business domain security techniques. It has only recently been understood that many of these traditional techniques break modern control systems and automation. Additionally, interconnection of the two types of enterprises represent substantial risks to each other because of their fundamentally different and incompatible nature.

Control System networks and enterprises must be designed and secured from a unique primary purpose perspective of machine and enterprise functionality, because the parallel computing environment that exists within ICS operation is fundamentally different than machine operation in a business environment. This even includes machines traditionally designated as "Clients" or "Servers". You can understand these differences more clearly by thinking of an ICS as a Peer-to-Peer Network model, though this is not strictly correct when applied to an ArchestrA Platform, for instance. This unique perspective requires looking at ICSs from a fresh viewpoint as compared with machines in a business environment, and understanding the unique needs involved with engineering a proper environment for them to operate in and securing that environment.

Because the machines in an ICS are Windows OS based, they are vulnerable to attacks on Windows Operating Systems just like in a business environment, but that is where the similarity ends. Many of the nuisance attacks that are normally tolerated and dealt with reactively inside a business domain simply can not be tolerated within an ICS domain. That is part of the reason for this manual. It is designed to reeducate you in how ICS machines interact, and the unique set of problems and issues that you will encounter when properly securing them.

During the past year, we have accumulated stories of plants going down due to attacks both inadvertent and intentional, resulting in anywhere from lost production to loss of life and irreversible environmental damage. The statistics on these incidents are terrifying, and everyone in the security industry is stating that the attacks and incidents will only get worse as time goes on.

On the surface, the techniques and procedures outlined herein look like a lot of work, however it has been proven by adopters of Secure ICSs that the ongoing administrative overhead and ongoing security costs were cut by an exponent when compared to the reactive security techniques currently employed and commonly used in business enterprises... and on top of that, some customers have reported that intentional attackers have even been stopped and prosecuted because of the techniques outlined in this manual. Surprisingly, over 50% of attacks last year (2005) to ICSs occur from inside the "trusted" business domain as reported by WurdTech, a security analysis firm.

Additionally, it has also been discovered that some security techniques and methodology (such as the belief that firewalls are "secure") utilized even a year ago have been badly eroded or entirely obsoleted in this ongoing battle. It is just an unfortunate fact recognized by experts in the ICS Security field that continued interconnectivity and direct interaction between business and ICS domains simply endangers each other from the standpoints of security and safety. Therefore, it is necessary to just break that connection- not necessarily physically, because it is simply not practical in many enterprises- and establish a proper security perimeter around this valuable equipment.

Reading through the case studies taken from the DHS archives in the beginning of the manual will give you some idea of a few pervasive security breach vectors that may exist in your organization. Applying any one of the scenarios to your ICS would spell a recipe for disaster-financially, environmentally, even possible injury or loss of life. In the past we as a society used to believe that people wouldn't intentionally do things that would hurt innocent bystanders. These case histories prove that this belief obviously isn't true anymore.

The ramifications of automation downtime and loss of control of industrial processes are just too great to be ignored anymore. Every day we read about new code such as rootkits, netbots, Nmap abuse, or VoMM (eVade o' Matic Module), that can surreptitiously infiltrate operating system modules through "secure" firewalls in business domains. We are also finding that intentionally secured domains such as banks or financial institutions containing personal information databases are increasingly being physically separated from their normal business domain environments in order to meet regulatory requirements of Sarbannes-Oxley, for one.

Why not with the ICS domains as well? Regulatory requirements for many critical infrastructure industries are already suggesting that this will likely be an outcome or requirement, probably by 2008, and so the guidance presented in this manual only makes sense to implement immediately. Already, government agencies containing ICSs (and their vendors) are subject to and will require compliance with NIST 800-53 (See the Appendix for more information).

Therefore the question only remains not, "Will we adopt these security techniques?" but, "WHEN will we adopt these security techniques?" Faced with the current challenges of today, right this minute, and what the security prospects look like even a year from now, this is a very good question, indeed.

Before You Begin

About This Document

This Securing Industrial Control Systems document provides recommendations and "best practice" information so that you can effectively define security needs and design and implement projects in a Wonderware® environment.

Recommendations included in this guide are derived from lab- and field-based experience gained from the development of security-related projects using the ArchestrA™ infrastructure for Wonderware Systems.

Recommendations and background information included in this document is derived from studies conducted by the [National Institute of Standards and Technology](#) (NIST). This content is included by express permission of the authors.

Audience

This document is written for Application and Process Engineers, IT Security Professionals, and System Integrators focused on plant security.

- Control engineers, integrators, and architects who design or implement secure SCADA or Industrial Control Systems (ICSs).
- System administrators, engineers, and other Information Technology (IT) professionals who administer, patch, or secure SCADA or ICSs.
- Security consultants who perform security assessments of SCADA or ICSs.
- Managers who are responsible for SCADA or ICSs.
- Researchers and analysts who are trying to understand the unique security needs of SCADA or ICSs.
- Vendors that are developing products that will be deployed as part of a SCADA or ICSs.
- IT Security Professionals who are involved with securing Automation, Process Control, and/or SCADA System domains, especially when integrating them into a larger corporate enterprises.

Assumptions

This document assumes familiarity with general computer security concepts and with using Web-based methods for retrieving information.

Familiarity with the working environment of the Microsoft Windows 2003 Server, and Windows XP/Vista operating systems, as well as with Virus protection software, Firewalls, Routers, switches, and Intrusion detection and prevention software is also assumed.

An understanding of concepts such as Active Directory, Group security, Group policy, and domain policy will help you to achieve the best results.

It is further assumed that you are familiar with Wonderware system components, and have an understanding of why control system domains are fundamentally different from business domains. For additional information about a specific component, see the *Wonderware FactorySuite A2 Deployment Guide*.

Document Conventions

This documentation uses the following conventions:

Convention	Used for
Bold	Menus, commands, buttons, icons, dialog boxes and dialog box options.
Monospace	Start menu selections, text you must type, and programming code.
<i>Italic</i>	Options in text or programming code you must type.

Where to Find Additional Information

Wonderware offers a variety of support options to answer questions on Wonderware products and their implementation.

Wonderware Security Central Website

Current up-to-date compatibility information is available on the Security Central Website

[<http://portal.wonderware.com/sites/securitycentral/default.aspx>] which contains Microsoft Critical Patches and associated (if any) changes that need to occur to Wonderware Software.

The site also offers RSS Feed subscription for Critical Updates and links for other websites and white papers that may affect your control system solutions.

ArchestrA Community Website

For timely information about products and real-world scenarios, refer to the ArchestrA Community website: <http://www.archestra.biz>. The ArchestrA Community website is a centralized information center where users, Systems Integrators (SIs) and OEMs can share information and application stories, obtain products and learn about training opportunities.

A key component of this website is the Application Object Warehouse, a constantly growing resource that provides downloadable ArchestrA objects, including a range of shareware products.

In the future, objects from the Invensys-driven object library will be available for purchase. Third parties are also encouraged to submit their own ArchestrA objects for inclusion.

Technical Support

Before contacting Technical Support, please refer to the appropriate chapter(s) in this manual and to the *User's Guide*, *Installation Guide* and Online Help for the relevant FactorySuite A² component(s).

For local support in your language, please contact a Wonderware-certified support provider in your area or country. For a list of certified support providers, refer to <http://us.wonderware.com/aboutus/contactsales>.

- **E-mail:** Receive technical support by sending an e-mail message to your local distributor or to support@wonderware.com.
- **Web:** You can access Wonderware Technical Support online at <http://www.wonderware.com/support/mmi>. Additionally, you can enter a new Service Request by using the website at <http://www.wonderware.com/support/mmi/esupport/AssistedSupport/Siebel753WebClient/SRInsert.aspx>.
- **Telephone:** You can call Wonderware Technical Support at the following numbers:
 - U.S. and Canada (toll-free): 800-WONDER1 (800-966-3371) 7 a.m. to 5 p.m. (Pacific Time)
 - Outside the U.S. and Canada: +1 (949) 639-8500

If you need to contact technical support for assistance, please have the following information available:

- The type and version of the operating system you are using. For example, Microsoft Windows XP Professional.
- The exact wording of the error messages encountered.
- Any relevant output listing from the Log Viewer or any other diagnostic applications.
- Details of the attempts you made to solve the problem(s) and your results.
- Details of how to recreate the problem.
- If known, the Wonderware Technical Support case number assigned to your problem (if this is an ongoing problem).

When requesting technical support, please include your first, last and company names, as well as the telephone number or e-mail address where you can be reached.

C H A P T E R 1

Industrial Control Systems Review

Industrial Control System (ICS) is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other smaller control system configurations often found in the industrial control sectors.

ICSs are used in the electric, water, oil and gas, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (automotive, aerospace, and durable goods) industries, to name but a few applications. This section provides an overview of SCADA and DCS systems, including typical architectures and components.

Contents

- SCADA and DCS Review

SCADA and DCS Review

SCADA systems are highly distributed systems used to control geographically dispersed assets, often scattered over thousands of square kilometers, where centralized data acquisition and control are critical to system operation. They are used in the distribution operations of water supply and wastewater systems, oil and 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. This includes monitoring alarms and processing status data. Based on information received from remote stations, automated or operator-driven supervisory commands can be pushed to remote station control devices, which are often referred to as field devices. Field devices control local operations such as opening and closing valves and relays, collecting data from sensor systems, and monitoring the local environment for alarm conditions.

DCSs are used to control manufacturing processes such as electric power generation, oil and gas refineries, and chemical, food, and automotive production. DCSs are integrated as a control architecture containing a supervisory level of control overseeing multiple, integrated sub-systems that are responsible for controlling the details of a localized manufacturing process. DCSs are used extensively in process-based and discrete-based manufacturing industries.

The two main types of process-based manufacturing are as follows:

- **Continuous Manufacturing Processes:** These processes run at a steady state condition, often with transitions to make different grades of a product. Typical continuous manufacturing processes include fuel or steam flow in a power plant, petroleum in a refinery, and distillation in a chemical plant.
- **Batch Manufacturing Processes:** Distinct processing steps, conducted on a quantity of material, characterize these processes. There is a distinct start and end step to a batch process with the possibility of brief steady state operations during intermediate steps.

The discrete-based manufacturing industries typically conduct a series of steps on a single device to create the end product. Electronic and mechanical parts assembly and parts machining are typical examples of this type of industry.

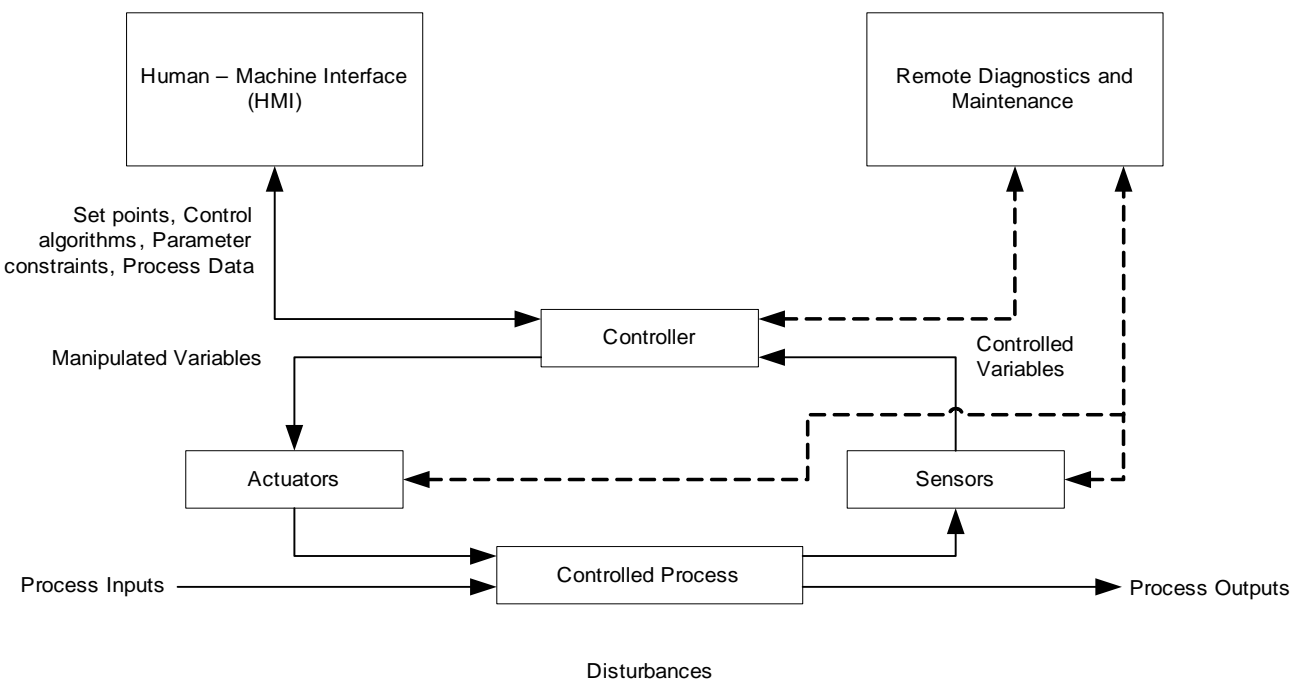
Both process-based and discrete-based industry segments utilize the same types of control systems, sensors, and networks.

NIST draft publication SP 800-82 contains detailed information on ICS Security Activities. This publication is located on the Drafts [<http://csrc.nist.gov/publications/drafts.html>] webpage of the Computer Security Division of the NIST Website [<http://csrc.nist.gov/>]. Once the document comes out of draft review, it will be available in entirety on the downloads page of the NIST website.

ICS Operation Review

The basic ICS operation is shown in the following graphic. Key Components include the following:

- **Control Loop:** A control loop consists of sensors for measurement, controller hardware, process actuators, and communication of variables. Controlled variables are transmitted to the controller from the process sensors. The controller interprets the signals and generates corresponding manipulated variables, based on set points, that it transmits to the process actuators. Process changes result in new sensor signals, identifying the state of the process, to again be transmitted to the controller.
- **Human-Machine Interface (HMI):** HMIs are used by operators and engineers to configure set points, control algorithms, and parameters in the controller. The HMI also displays process status information and historical information.
- **Remote Diagnostics and Maintenance Utilities:** Diagnostics and maintenance utilities are used to identify, prevent and recover from failures.



A typical ICS contains a proliferation of control loops, HMIs, and remote diagnostics and maintenance tools built using an array of network protocols and layered network architectures. Supervisory-level loops and lower-level loops operate continuously over the duration of a process with cycle times ranging on the order of milliseconds to minutes.

Key ICS Components

This section defines key ICS components that are used in control and networking. Some of these components can be described generically for use in both SCADA systems and DCSs, while others are unique to one.

Key Control Components

The following is a list of the major control components of an ICS:

- **Control Server:** The control server hosts the DCS supervisory control software that is designed to communicate with lower-level control devices. The control server accesses subordinate control modules over a facilities control network.
- **SCADA Server or Master Terminal Unit (MTU):** This is the device that acts as the master in a SCADA system. This master device is assigned the right to transmit. Remote terminal units and programmable logic controller slave devices (described below) located at remote field sites act as slaves.
- **Remote Terminal Unit (RTU):** Also called a Remote Telemetry Unit, an RTU is a special purpose standalone data acquisition and control unit designed to support SCADA remote stations. RTUs are field devices often equipped with wireless radio interfacing to support remote situations where wire-based communications are unavailable. Sometimes programmable logic controllers (PLC) are implemented as field devices to serve as RTUs; in this case, the PLC is often referred to as an RTU.
- **Programmable Logic Controller (PLC):** The PLC is a small industrial computer originally designed to perform the logic functions executed by electrical hardware (relays, drum switches, and mechanical timer/counters). PLCs have evolved into controllers of complex processes, and they are used substantially in SCADA systems and DCSs.

Other controllers used at the field level are process controllers and RTUs that provide the same control as PLCs but are designed for specific control applications. In SCADA environments, PLCs are often used as field devices because they are more economical, versatile, flexible, and configurable when compared to special-purpose RTUs.

- **Intelligent Electronic Devices (IED):** These are "smart" sensors containing the intelligence required to acquire data, communicate to other devices, and perform local processing. An IED could combine an analog input sensor, analog output, low level control capabilities, a communication system, and program memory on one device.

- **Human-Machine Interface (HMI):** HMI is software and hardware that enables human operators to monitor the state of a process under control, modify control settings to change the control objective, and manually override automatic control operations in the event of an emergency. The HMI also allows a control engineer or operator to configure set points or control algorithms and parameters in the controller.

The HMI also displays process status information, historical information, reports, and other information to operators, administrators, managers, business partners, and other authorized users. The location, platforms and interfaces may vary a great deal. For example, an HMI could be a dedicated platform in the control center, a laptop on a wireless LAN, a tablet computer, or a browser on any system connected to the Internet.

- **Historian:** The Historian is a centralized database for logging all process information within an ICS. Process information from this database can be accessed to support various business analyses, from statistical process control to enterprise level planning.
- **Input/Output (I/O) Servers:** The I/O server is a control component responsible for relaying information sent between control servers and control sub-components such as PLCs and IEDs. An I/O server can reside on the control server or on a separate computer platform. I/O servers are also used for interfacing third-party control components, such as an HMI and a control server.

Key Network Components

Each layer within a control system hierarchy has different network characteristics. Network topologies across different SCADA and DCS implementations vary with modern systems using Internet-based IT and enterprise-integration strategies. Control networks have merged with enterprise networks to allow engineers to monitor and control systems from outside of the control system network.

The enterprise connection also allows enterprise-level decision-makers to obtain instant access to process data. The following is a list of the major components of an ICS network, regardless of the network topology:

- **Fieldbus Network:** This network links sensors and other devices to a PLC or other controller. Using fieldbus technologies eliminates the need for point-to-point wiring between the controller and each device. Sensors communicate with the fieldbus controller using a specific protocol. Messages sent between the sensors and the controller uniquely identify each of the sensors.
- **Control Network:** Also called a peer-to-peer network, the control network connects the supervisory control level to lower-level control modules within a DCS.
- **Communications Routers:** A router is a communications device that transfers messages between two networks. Common uses for routers include connecting a LAN to a WAN, and connecting MTUs and RTUs to a long distance network medium for SCADA communication.

- **Firewall:** The firewall protects devices on a network by monitoring and controlling communication packets using predefined filtering policies. Firewalls are also useful in managing ICS network segmentation strategies.
- **Modems:** Modems convert serial digital data to a digital signal suitable for transmission over a telephone line for device communication. Modems are often used in SCADA systems to enable long distance serial communications between MTUs and remote field devices. They are also used in both SCADA systems and DCSs for gaining remote access for operational functions and for diagnostic purposes.
- **Remote Access Points:** These are mechanisms for remotely configuring systems and accessing process data. Examples include using a personal digital assistant (PDA) to access data over a LAN through a wireless access point, and using a laptop and modem connection to remotely access an ICS system.

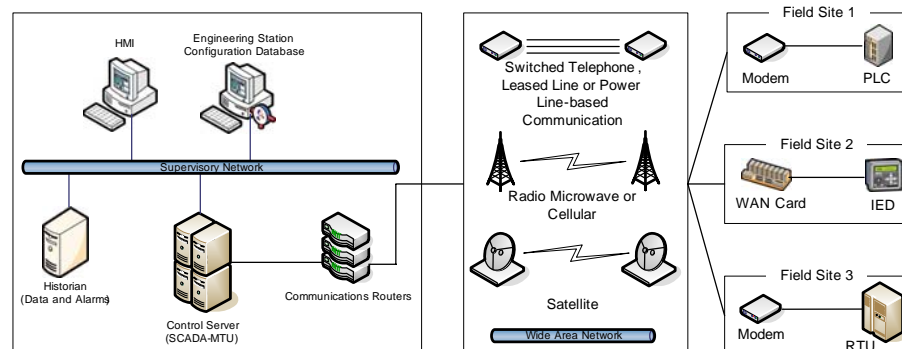
SCADA System Review

SCADA systems are used to control dispersed assets where centralized data acquisition is as important as control. These systems are used in the distribution operations of water supply and wastewater systems, oil and gas pipelines, electrical systems and rail systems. SCADA systems integrate data acquisition systems with data transmission systems and HMI software to provide a centralized monitoring and control system for numerous process inputs and outputs.

SCADA systems are designed to collect field information, transfer it to a central computer facility, and display the information to the operator graphically or textually, thereby enabling system monitoring/control from a central location, in real time.

Based on the sophistication and setup of the individual system, control of any individual system, operation, or task can be automatic, or it can be initiated by operator commands.

The following graphic shows the components and general configuration of a SCADA system:

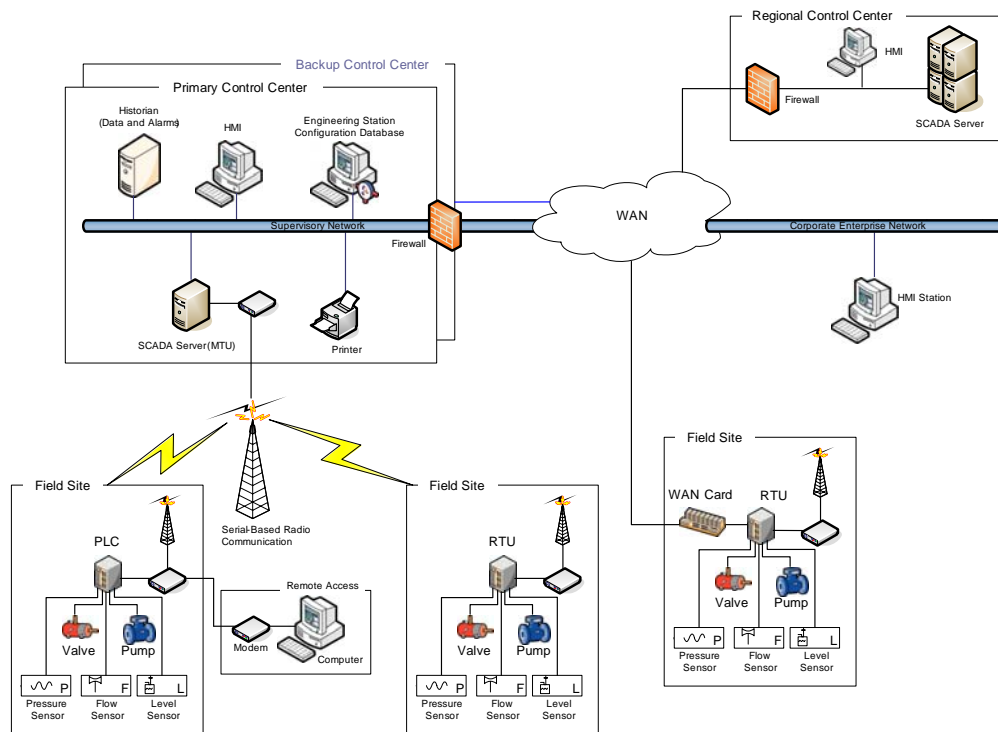


The **Primary Control Center** houses a control server (MTU) and the communications routers. Other Control Center components include the HMI, engineering workstations, and the data historian, which are all connected by a LAN. The Control Center collects and logs information gathered by the field sites, displays information to the HMI, and generates actions based upon detected events. The Control Center is also responsible for centralized alarming, trend analyses, and reporting.

The **Field Site** performs local control of actuators and monitors sensors. Field Sites are often equipped with a remote access capability to allow field operators to perform remote diagnostic and repair.

SCADA Topology

The following graphic describes a typical SCADA system implementation:



This typical SCADA system consists of the following characteristics:

- A primary control center and three field sites.
- A second backup control center provides redundancy in the event of a primary control center malfunction.
- Point-to-point connections are used for all control center to field site communications, with two connections using radio telemetry.
- The third field site is local to the control center and uses the wide area network (WAN) for communications.
- A regional control center sits above the primary control center for a higher level of supervisory control.

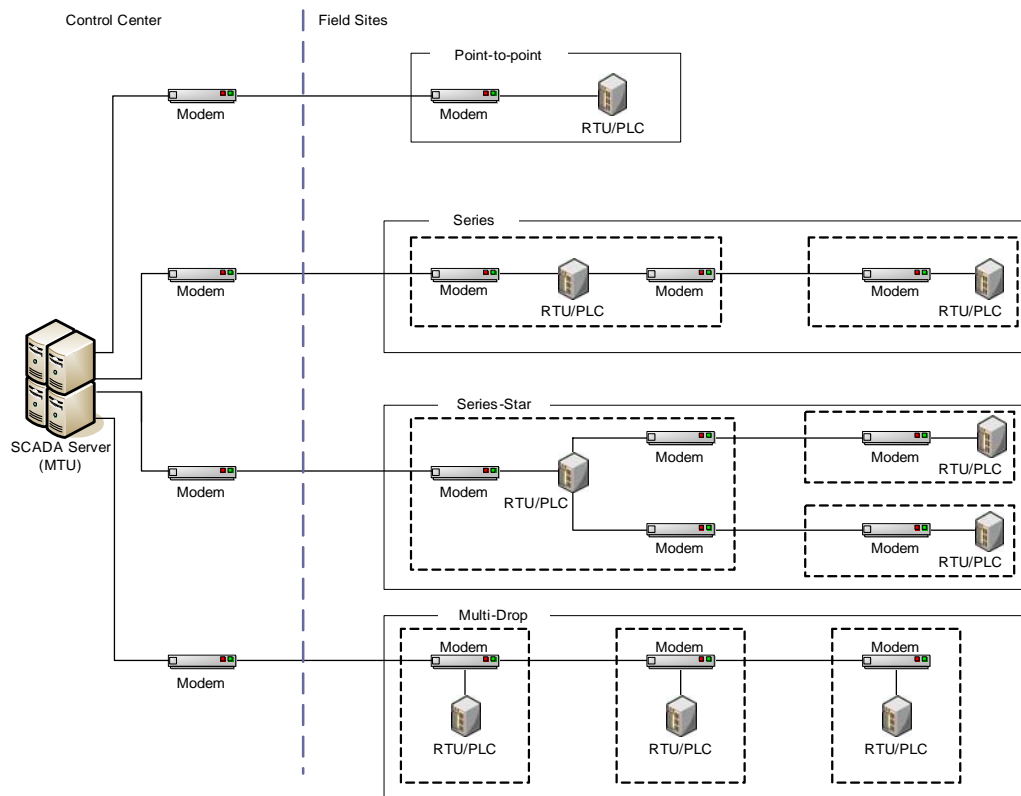
- The corporate enterprise network has access to all control centers through the WAN, and field sites can be accessed remotely for troubleshooting and maintenance operations.
- The primary control center polls field devices for data at five-second intervals and can send new set points to a field device as required.

In addition to polling and issuing high level commands, the SCADA server also watches for priority interrupts coming from field site alarm systems.

SCADA System Communication Implementation

Standard and proprietary communication protocols (run over serial communications) transport information between the Control Center and Field Sites using telemetry techniques such as telephone line, cable, or radio frequencies.

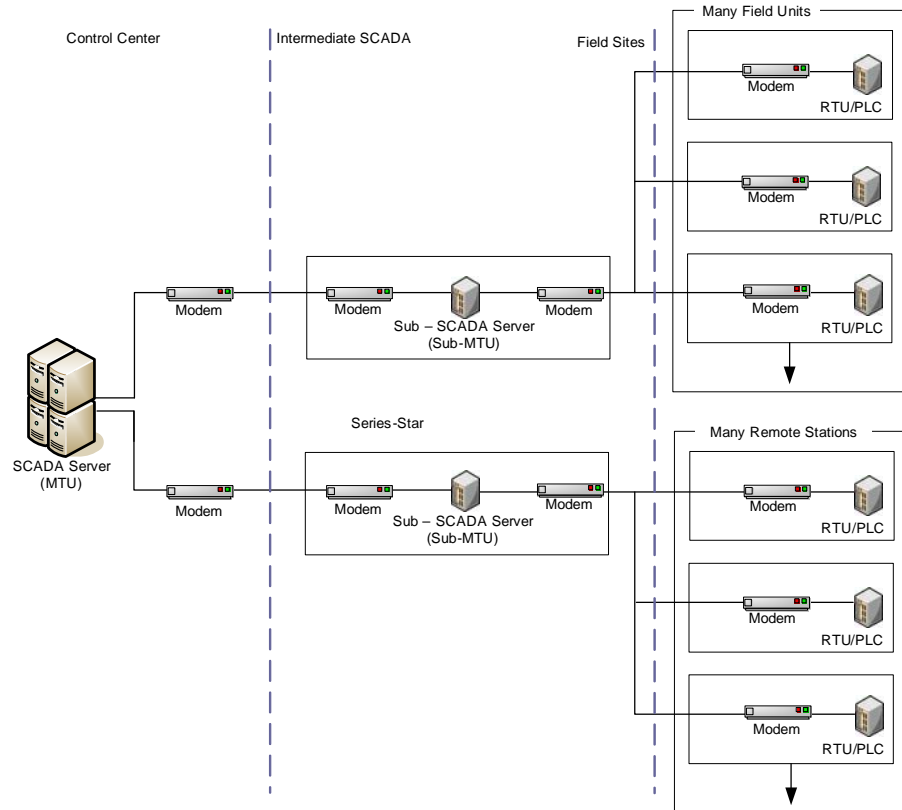
The following graphic describes various MTU-RTU communication architecture implementations. It includes point-to-point, series, series-star, and multi-drop:



Point-to-point is functionally the simplest type; however, it is expensive because of the individual channels needed for each connection. In a series configuration, the number of channels used is reduced; however, channel sharing has an impact on the efficiency and complexity of SCADA operations. Similarly, the series-star and multi-drop configurations' use of one channel per device results in decreased efficiency and increased system complexity.

The four basic architectures shown in the previous graphic can be further augmented using dedicated communications computers to manage communication exchange, as well as message switching and buffering.

Large SCADA systems, containing hundreds of RTUs, often employ sub-MTUs to alleviate the burden on the primary MTU. This implementation is described in the following figure:



SCADA System Key Components Summary

SCADA systems consist of both hardware and software. Typical hardware includes:

- An MTU placed at a control center
- Communications equipment (radio, telephone line, cable, or satellite),
- One or more geographically distributed field sites consisting of either an RTU or a PLC, which controls actuators and/or monitors sensors.

The MTU stores and processes the information from RTU inputs and outputs, while the RTU or PLC controls the local process. The communications hardware allows the transfer of information and data back and forth between the MTU and the RTUs or PLCs.

The software tells the system what and when to monitor, what parameter ranges are acceptable, and what response to initiate should the parameters go outside acceptable ranges.

An IED, such as a protective relay, may communicate directly to the SCADA master station, or a local RTU may poll the IEDs to collect the data and pass it to the SCADA master station. IEDs provide a direct interface to control and monitor equipment and sensors. IEDs can be directly polled and controlled by the SCADA master station and may have local programming that allows for the IED to act without direct instructions from the SCADA control center. SCADA systems are designed to be fault-tolerant systems with significant redundancy built into the system architecture.

Distributed Control Systems Review

DCSs are used to control production systems within the same geographic location for businesses such as oil and gas refineries, electric power generation plants, chemical plants, automobile production facilities and food and pharmaceutical processing facilities. These systems are usually process control or discrete part control systems.

A DCS uses a centralized supervisory control loop to mediate a group of localized controllers that share the overall tasks of carrying out an entire production process. By modularizing the production system, a DCS reduces the impact of a fault on the overall system. In most systems, the DCS interfaces with the enterprise level of a production facility to give business operations a view of production.

Control systems used in distribution and manufacturing industries are very similar in operation. However, one of the primary differences is the fact that DCS-controlled sub-systems are usually located within a more confined factory- or plant-centric area, when compared to geographically dispersed SCADA field sites.

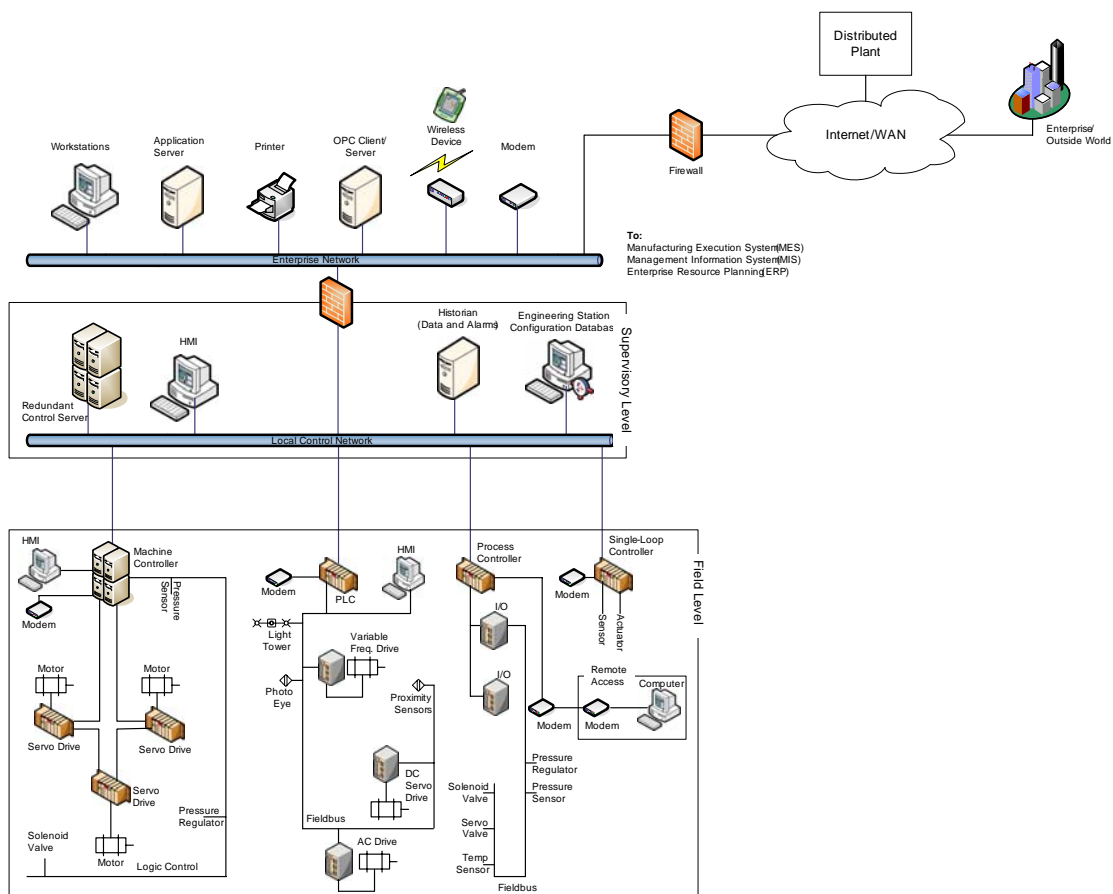
DCS communications are usually performed using local area network (LAN) technologies that are typically more reliable and high speed compared to the long distance communication systems used by SCADA systems. In fact, SCADA systems are specifically designed to handle long distance communication challenges such as delays, and data loss posed by the various communication media used.

DCS systems usually employ greater degrees of closed loop control than SCADA systems since control of manufacturing processes are typically more complicated compared to the control of a distribution process.

These differences can be considered subtle for the scope of this document that focuses on the integration of information technology (IT) security into these systems. Throughout the remainder of this document, SCADA systems and DCSs will be referred to as ICS unless a specific reference is made to one (e.g., field device used in SCADA systems).

DCS System Topology

The following graphic describes an example implementation, and includes the components and general configuration of a DCS:



This DCS encompasses an entire facility from the bottom level production processes, up to the business or enterprise layer. In this example, a supervisory controller (control server) communicates to its subordinates via a control network. The supervisor sends set points to and requests data from the distributed field controllers.

The distributed controllers control their process actuators based on control server commands and sensor feedback from process sensors.

Key Low-Level Controller Components

The previous graphic also shows examples of low-level controllers found on a DCS system.

The field control devices include a PLC, a process controller, a single loop controller, and a machine controller with the following functionality:

- The single loop controller interfaces sensors and actuator using point-to-point wiring.
- The other three field devices incorporate fieldbus networks to interface with process sensors and actuators. Fieldbus networks eliminate the need for point-to-point wiring between a controller and individual field sensors and actuators. Standard industrial communication protocols designed by industry groups such as Modbus and Fieldbus are often used on control networks and fieldbus networks.

In addition to supervisory-level and the field-level control loops, intermediate levels of control may also exist. For example, in the case of a DCS controlling a discrete part manufacturing facility, there could be an intermediate level supervisor for each cell within the plant. This supervisor would encompass a manufacturing cell containing a machine controller that processes a part and a robot controller that handles raw stock and final products. There could be several of these cells that manage field level controllers under the control of the main DCS supervisory control loop.

SCADA and DCS Examples by Industry

Industries using include the electrical power transmission and distribution grids use geographically-distributed SCADA control technology, which relies on highly-interconnected networks, and includes dynamic systems consisting of thousands of public and private utilities and rural cooperatives that supply electricity to end users.

In this example, the SCADA system manages electricity distribution by collecting data from, and issuing commands to, geographically-remote field control stations from a centralized location.

SCADA systems are also used to control oil and gas distribution, including pipelines, ships, trucks, and rail systems. A wastewater treatment infrastructure is very similar to that of a water supply infrastructure and also uses SCADA systems for control.

SCADA systems and DCSs are often tied together. This is the case for electric power distribution and electric power generation facilities. Although the electric power generation facility operation is controlled locally by a DCS, the DCS must communicate with the SCADA system to coordinate production output with distribution demands.

The U.S. critical infrastructure is often referred to as a "system of systems" because of the interdependencies that exist between its various industrial sectors. Critical infrastructures are highly-interconnected and mutually-dependent in complex ways, both physically and through a host of information and communications technologies.

What happens to one infrastructure can directly and indirectly affect other infrastructures through cascading and escalating failures.

Electric power is considered to be one of the most prevalent primary source critical infrastructures causing disruptions of interdependent critical infrastructures. For example, a cascading failure can be initiated by a disruption of the microwave communications network used for the SCADA system of an electric power distribution system.

The resultant lack of monitoring and control capabilities can cause a large generating unit to be taken offline. This event would then cause a loss of power at a distribution substation. The power loss can cause a major imbalance that would trigger a cascading failure across the power grid.

The final result is a large area blackout that affects oil and natural gas production, refinery operations, water purification systems and the pipeline transport systems for these resources.

ICS System Review Summary

Industrial control systems (ICS), which include supervisory control and data acquisition (SCADA) systems and distributed control systems (DCS), are used in the electric, water, oil and gas, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (automotive, aerospace and durable goods) industries.

SCADA systems are used to control dispersed assets using centralized data acquisition and control. DCSs are used to control production systems within a local area such as a factory.

These control systems are critical to the operation of the U.S. critical infrastructures that are often highly interconnected and mutually dependent systems both physically and through a host of information and communication technologies.

C H A P T E R 2

Defining ICS Security Risk Areas

Most ICSs were developed long before public and private networks, desktop computing, or the Internet were a common part of business operations. These systems were designed to meet performance, reliability, safety, and flexibility requirements.

In most cases they were physically isolated from any outside networks and based on proprietary hardware, software, and communication protocols that included basic error detection and correction capabilities, but lacked the secure communications. The need for cyber-security measures within these systems was not anticipated. Security for ICS meant securing physical access to the network and the consoles that controlled the systems.

As microprocessor, personal computer, and networking technology evolved during the 1980s and 1990s, ICS design changed to incorporate the latest technologies. Internet-based technologies started making their way into ICS designs in the late 1990s. These changes to ICSs exposed them to new types of threats and significantly increased the likelihood that they could be attacked.

This chapter describes the unique security characteristics of ICSs, the vulnerabilities in ICS implementations, and the threats and attacks that ICSs may face. The end of the section presents several examples of actual ICS attack incidents.

This chapter describes the security risk areas that should be reviewed before implementing an industrial control system.

Contents

- ICS and IT System Risk Overview
- Assessing Security Risks
- Assessing ICS Vulnerabilities
- Security Threats and Attack Scenarios
- Detecting and Preventing Insider Threats

ICS and IT System Risk Overview

Until recently, ICSs had little resemblance to business IT systems because they were isolated systems running proprietary control protocols. As these systems are integrated with IT solutions to promote corporate connectivity and remote access capabilities, they begin to resemble IT systems.

This integration supports new IT capabilities, but provides significantly less isolation for ICSs from the outside world than predecessor systems. While security solutions have been designed to deal with these security issues in typical IT systems, special precautions must be taken when introducing these same solutions to ICS environments. In some cases, new IT security solutions are needed.

ICS and IT System Risk Comparison and Analysis

ICSs are functionally different than traditional Internet-based information processing systems, and include very different risks and operational priorities. For example, ICS risk factors include significant risk to the health and safety of human lives, serious damage to the environment, financial issues (such as production losses, negative impact to a nation's economy), and compromising proprietary information.

ICSs also have different performance and reliability requirements and use operating systems and applications that may be considered unconventional to typical IT personnel. Furthermore, the goals of safety and security sometimes conflict in the design and operation of control systems.

ICS Operational Requirements Summary

The following items are special considerations when considering security for ICSs:

- **Performance Requirements:** ICSs are generally time critical; delay is not acceptable for the delivery of information, and high throughput is typically not essential.
- **High-Availability Requirements:** Many ICS processes are continuous in nature. Unexpected outages of systems that control industrial processes are not acceptable. Exhaustive pre-deployment testing is essential to ensure high availability for the ICS.

In addition to unexpected outages, many control systems cannot be easily stopped and started without affecting production. In some cases, the products produced or equipment being used is more important than the information being relayed.

- **Risk Management Requirements:** Human safety and fault tolerance (to prevent loss of life or endangerment of public health or confidence), loss of equipment, loss of intellectual property, or lost or damaged product are the primary concerns. The personnel responsible for operating, securing, and maintaining these systems must understand the link between safety and security.

- **Architecture Security Focus:** ICS "edge" devices (e.g., PLC, operator station, DCS controller) must be more carefully protected since they are directly responsible for controlling the end process. The protection of the central server is still very important in an ICS, since the central server could possibly control every edge device.
- **Unintended Consequences:** ICSs can have very complex interactions with physical processes. All security functions integrated into the process control system must be tested to prove that they do not introduce unacceptable vulnerabilities. Adding any physical or logical security components to the system may reduce the reliability of the control system, but the resulting reliability should be kept to acceptable levels.
- **Time Critical Responses:** For some ICS, automated response time or system response to human interaction is critical. For example, emergency actions for industrial control systems should not be hampered by requiring password authentication and authorization. Information flow must not be interrupted or compromised. Access to these systems should be restricted by rigorous physical security controls.
- **System Software:** ICS networks are (typically) more complex and require a different level of expertise (i.e., control networks are typically managed by control engineers, not IT personnel). Software and hardware applications are more difficult to upgrade in a control system network. Many systems may not have desired features, including encryption capabilities, error logging, and password protection.
- **Resource Constraints:** Control systems and their real time OSs are resource-constrained systems that usually do not include typical IT security technologies. Computing resources are not always available to retrofit these systems with current security technologies.
- **Communications:** Communication protocols and media used by ICS environments are typically different from the generic IT environment, and may be proprietary.
- **Software Updates:** Change management is paramount to maintaining the integrity of both IT and control systems. Software updates on ICSs cannot always be implemented on a timely basis because their changes need to be thoroughly tested by both the industrial control application vendor and by the end user before being implemented. In addition, this change management process, when applied to ICSs, requires careful assessment by ICS experts working in conjunction with security and IT personnel.

ICN and IT Operational Requirements Summary Comparison

The following table puts these ICS operational requirements into context by comparing them with standard IT Operational Requirements:

Category	ICS Requirements	IT Requirements
Performance	<ul style="list-style-type: none"> • Real-time. • Response is time critical. • Modest throughput acceptable. • High delay and/or jitter is a serious concern. 	<ul style="list-style-type: none"> • Non-real-time. • Response must be reliable. • High throughput demanded. • High delay and jitter accepted.
Availability	<ul style="list-style-type: none"> • Unexpected system outages are not acceptable. • High availability requires exhaustive pre-deployment testing. 	<ul style="list-style-type: none"> • IT strategies such as rebooting are acceptable. • Availability deficiencies can be tolerated.
Risk Management	<ul style="list-style-type: none"> • Human safety is paramount. • Fault tolerance is essential, downtime is not acceptable. • Major risk impact is loss of life, equipment or product. 	<ul style="list-style-type: none"> • Data confidentiality and integrity is paramount. • Fault tolerance is not required, downtime is not a major risk. • Major risk impact is loss of business operations.
Security	Primary goal is to protect edge clients (i.e., field devices such as process controllers)	Primary goal is to protect the central server.
Unintended Consequences	Security tools must be tested to ensure that they do not introduce vulnerabilities or cause adverse effects to ICS operation.	Security solutions are designed around typical IT systems.
Time-Critical Interaction	<ul style="list-style-type: none"> • Response to human and other emergency interaction is critical. • Access to ICS should be rigorous, yet not hamper the flow of information. 	<ul style="list-style-type: none"> • No critical emergency interaction. • Access control can be implemented to the degree necessary.
System Software	<ul style="list-style-type: none"> • Differing and custom operating systems. • Software more difficult to upgrade in an ICS network. 	<ul style="list-style-type: none"> • Systems designed for use with typical operating systems. • Upgrades are straightforward with the availability of automated deployment tools.
Resource Constraints	Designed to support the intended industrial process, with minimal memory and computing resources to support the addition of security technology.	Systems are specified with enough resources to support the addition of third-party applications such as security solutions.

Category	ICS Requirements	IT Requirements
Communications	<ul style="list-style-type: none"> • Many proprietary communication protocols. • Several types of communications mediums used. • Networks are complex and sometimes require the expertise of control engineers. 	<ul style="list-style-type: none"> • Standard communications protocols. • Primarily wired networks with some localized wireless capabilities. • Typical IT networking practices.
Software Updates	Software changes must be thoroughly tested and deployed incrementally throughout a system to ensure that the control systems' integrity is maintained. Because of this requirement, security patches cannot always be implemented on a timely basis.	Software changes are applied in a timely fashion in the presence of good security policy and procedures. The procedures are often automated.

Requirements Comparison Summary

The operational and risk differences between ICS and IT systems create the need for different IT security strategies within the ICS environment:

- The primary goal of Internet business systems is to protect the central server, while with ICS environments, it is the edge clients such as PLCs and process controllers that must be protected, rather than an information server such as a data historian server.
- Available computing resources for ICSs (including central processing unit [CPU] time and memory) tend to be very limited because these systems were designed to maximize control system resources, with little to no extra capacity for third-party IT security solutions.
- IT security and control systems expertise are typically not found within the same group of personnel. A cross-functional team of control engineers and IT professionals must work closely (cooperatively) to understand the possible implications of the installation, operation, and maintenance of security solutions in conjunction with control system operation.

IT professionals working with ICSs need to understand the reliability impacts of information security technologies *before* deployment. Some of the OSs and applications running on ICSs may not operate correctly with off-the-shelf IT solutions because of specialized ICS environment architectures.

Note For a detailed discussion on machine roles and other ICS security considerations, see "Security Perspective" on page 158.

Assessing Security Risks

The following ICS implementation trends have increased overall security risks to control systems:

- Wide adoption of Standardized Protocols and Technologies with known vulnerabilities.
- Increased Connectivity of the control systems to other networks.
- Insecure and Rogue Connections (unknown remote connections).
- Public Information (widespread availability of technical information) about control systems.

Standardized Protocols and Technologies

ICS vendors are opening up their proprietary protocols, and publishing their protocol specifications in order to enable third-party manufacturers to build compatible accessories. Organizations are also transitioning from proprietary systems to less expensive, standardized technologies such as Microsoft Windows and Unix-like operating systems, as well as common networking protocols such as TCP/IP to reduce costs and improve performance.

Another standard contributing to this evolution of open systems is Object Linking and Embedding (OLE) for Process Control (OPC), a protocol that enables interaction between control systems and PC-based application programs.

The transition to using these open protocol standards provides economic and technical benefits, but also increases the vulnerability to cyber-attack. These standardized protocols technologies have commonly known vulnerabilities, and sophisticated and effective exploitation tools that are widely available and relatively easy to use.

As a consequence, both the number of people with the knowledge to wage attacks and the number of systems subject to attack has increased. These common communication protocols also enable hackers to easily interpret the content of communications among the components of a control system.

Increased Connectivity

ICS and enterprise IT systems are often bridged as a result of two key changes in information management practices:

- First, the demand for remote access has encouraged many organizations to establish connections to the ICS that enable ICS engineers to monitor and control the system from points on the corporate network.

- Second, many organizations have added connections between corporate networks and ICS networks to allow the organization's decision makers to obtain instant access to critical data about the status of their operational systems. In early implementations this might have been done with custom applications software or via an OPC server/gateway; however, in the past ten years this has been accomplished with Transmission Control Protocol/Internet Protocol (TCP/IP) networking, and standardized IP applications like File Transfer Protocol (FTP) or Extensible Markup Language (XML) data exchanges.

Often, these connections were implemented without a full understanding of the corresponding security risks. In addition, corporate networks are often connected to strategic partner networks and to the Internet.

- Control systems also make more use of WANs and the Internet to transmit data to their remote or local stations and individual devices.

The integration of control system networks with public and enterprise networks increases control system security vulnerabilities. Unless appropriate security controls are deployed, these vulnerabilities can expose all levels of the ICS network architecture to attackers and a variety of cyber attacks, including worms and other malware.

As an example of the change in threats to control systems, an internal survey of an unnamed energy company showed the following:

- The majority of the business units' management believed their control systems were not connected to the business network.
- An audit showed the majority of systems were connected in some way to the business network.
- The business network was only secured to support general business processes, and not safety-critical systems.

Insecure and Rogue Connections

Many ICS vendors deliver systems with dial-up modems that provide remote access, in order to ease the burdens of technical field support personnel. Remote access provides support staff with administrative-level access to a system using a telephone number, a valid ID, and a password.

Attackers with war dialers—simple personal computer programs that dial consecutive phone numbers looking for modems—and password cracking software can gain access to systems through these remote access capabilities. These capabilities can leave a system highly vulnerable since people entering systems through vendor-installed modems are often granted high levels of system access.

Organizations often inadvertently omit access links (such as dial-up modems open for remote diagnostics, maintenance, and monitoring) from security evaluations. Further, control systems utilize wireless communications systems and commercially-facilitated leased lines, which are especially vulnerable to attack.

Access links without authentication and encryption increase the risk of attackers using these insecure connections to break into remotely controlled systems.

Many of the interconnections between corporate networks and ICS require integrating systems with different communications standards.

Network engineers often fail to account for security risks when integrating disparate systems. Access controls designed to protect control systems from unauthorized access through corporate networks are usually minimal or may not exist. This is because it is difficult to identify all the key access points connecting these networks.

Public Information

Public information regarding design, maintenance, interconnection, and communication is readily available over the Internet to support competition in product choices as well as to enable the use of open standards. ICS vendors also sell toolkits to help develop software that implements the various standards used in ICS environments. There are also many former employees, vendors, contractors, and other end users of the same ICS equipment worldwide who have inside knowledge about the operation of control systems.

Information and resources are available to potential attackers and intruders of all calibers. With the available information, it is quite possible for an individual with very little knowledge of control systems to gain unauthorized access to a control system with the use of a port scanning tool and the factory-set default password. Many times, these default passwords are never changed.

Potential ICS Vulnerabilities

This section lists vulnerabilities that may be found in typical ICSs. The order of these vulnerabilities does not necessarily reflect any priority in terms of likelihood of occurrence or severity of impact. The vulnerabilities are grouped into Policy and Procedure, Platform, and Network categories to assist in determining optimal mitigation strategies.

Any given ICS will usually exhibit a subset of these vulnerabilities, but may also contain additional vulnerabilities unique to the particular ICS implementation that do not appear in this listing. Specific information on ICS vulnerabilities can be found at the United States Computer Emergency Readiness Team (US-CERT) website <http://www.us-cert.gov/>

When studying possible security vulnerabilities, it is easy to become preoccupied with trying to address issues that are technically interesting, but are ultimately of low risk to the system. Therefore, a method for assessing and rating the risk of a possible vulnerability at a specific facility is needed. The risk is a function of the likelihood (probability) that a defined threat can exploit a specific vulnerability and set of consequences. The risk induced by any given vulnerability is influenced by a number of related indicators, including:

- Site architecture and conditions
- Installed countermeasures
- Technical difficulty of attack
- Probability of apprehension
- Cost of attack.

Assessing ICS Vulnerabilities

A review of existing IT policies and procedures provides information about what improvements or changes must occur for Process control.

For example, physical security is the first defense in any secure environment. The existing infrastructure and new infrastructure components play an integral part in that security. A detailed review reveals definition changes or improvements that must be made to secure the physical system.

The approach to site network(s) and control system security should be based on the following principles:

- View security from both management and technical perspectives.
- Ensure security is addressed from both an IT and control system perspective to include dedicated network devices and software configuration.
- Design and develop multiple layers of network, system and application security.
- Ensure industry, regulatory and international standards are taken into account.
- Prevention is critical in plant control systems, supported by detection.

Process control systems and networks are often implemented in pieces. Most have no consistent security design and many were not designed with security when they were designed. Threats from both internal and external sources have increased significantly.

Planning the secure environment includes the following focus areas:

- Policies and Procedures
- Platform Security
- Infrastructure Assessment
- Software

Policies and Procedures

Vulnerabilities are often introduced into ICSs because of incomplete or nonexistent security documentation, including policy and implementation guides (procedures).

Security documentation is the cornerstone of any security program. Corporate IT policy can reduce vulnerabilities by mandating conducts such as password usage and maintenance or requirements for connecting modems to ICSs.

The first task in building a solid defense against unwanted intrusion into business network and process control systems is to develop a security policy statement. The statement must define the requirements to implement a secure process environment. Once security goals are clear, a detailed plan can be developed to implement security.

Security policies and procedures are the foundation of a solid security strategy. Many automation, control, and access areas must have well defined security policies and procedures in place. The policies and procedures (and their enforcement) have a profound effect on success and future evolution of a secured control system environment.

Effective security Policies and Procedures development, management, and enforcement can be very difficult. However, a proactive network and system security approach can provide an effective security program that continues to work over time.

The following table summarizes Policies and Procedures Vulnerabilities in the ICN environment:

Vulnerability	Description
Inadequate security policy for the ICS.	Vulnerabilities are often introduced into ICSs due to inadequate policies, or the lack of policies specifically for control system security.
No formal security training program.	A documented formal security training program is designed to keep staff up to date on company security policies and procedures. Without training on policies and procedures, staff cannot be expected to maintain a secure ICS environment.
No specific or documented security procedures were developed from the security policy.	Specific security procedures must be developed for the ICS. They are the root of a sound security program.
Absent or deficient equipment implementation guidelines.	Equipment implementation guidelines must be kept up to date and readily available. These guidelines are an integral part of security procedures in the event of an ICS malfunction.
Lack of administrative mechanisms for security enforcement.	Staff must be held accountable for administering documented security policies and procedures.
Few or no security audits.	Independent security audits must review and examine a system's records and activities to determine the adequacy of system controls and ensure compliance with established security policy and procedures. Audits must also be used to detect breaches in security services and recommend changes as countermeasures.

Vulnerability	Description
No specific disaster recovery plan.	A disaster recovery plan is needed in the event of a major hardware or software failure or destruction of facilities. Lack of a specific disaster recovery plan for the ICS could lead to extended downtimes.
Lack of configuration change management.	A process for controlling modifications to hardware, firmware, software, and documentation must be implemented to ensure an ICS is protected against inadequate or improper modifications before, during, and after system implementation. A lack of configuration change management procedures can lead to security oversights, exposures, and risks.

The following information describes critical security element considerations:

User Accounts

A user account defines the actions a user can perform in Windows. On a stand-alone computer or a computer that is a member of a workgroup, a user account establishes the privileges assigned to each user. On a computer that is part of a network domain, a user must be a member of at least one group. The permissions and rights granted to a group are then assigned to its members.

The tendency to give users Administrative rights on their client computers greatly increases the risks from malicious software. The result of this permission is that when a user or administrator logs on with Administrative rights, any programs that they run, such as browsers, e-mail clients, and instant messaging programs, also have administrative rights.

If these programs activate malicious software, that malicious software can install itself, manipulate services such as antivirus programs, and even hide from the operating system. Users can run malicious software unintentionally and unknowingly, for example, by visiting a compromised Web site or by clicking a link in an e-mail message.

A defense-in-depth strategy, with overlapping layers of security, is the best way to counter these threats, and the Least-privileged User Account (LUA) approach is an important part of that defensive strategy. The LUA approach ensures that users follow the principle of least privilege and always log on with limited user accounts. This strategy also aims to limit the use of administrative credentials to administrators, and then only for administrative tasks.

The LUA approach can significantly mitigate the risks from malicious software and accidental incorrect configuration. However, because the LUA approach requires organizations to plan, test, and support limited access configurations, this approach can generate significant costs and challenges. These costs can include increased review and planning overhead, redevelopment of custom programs, changes to operational procedures, and deployment of additional tools.

User Accounts

User Accounts within a system must be dictated by strong security policies made up of useful account creation and maintenance procedures.

The policies that govern system accounts need to be fully thought through by IT, Automation Engineering, and Management.

Once documented, the procedures that implement the account policies must be published and presented to all users of the automation system. Listed below are a few things to consider when developing or reviewing account policies.

- Only validated users should have accounts.
- Users ID's have unique names with strong passwords.
- Individuals are accountable for the use of their user ID.
- User access should be restricted as much as possible (LUA).
- Make sure that account lockout duration is well defined.
- Groups should be defined by user access needs and roles.
- Guest accounts and default Vendor accounts should be removed or reset as applicable.
- Process Operator station accounts should be limited and defined by operational area.
- Service accounts should be on the local Domain or local machine and should not be used to logon to a server.

Passwords

Passwords are one of the most vulnerable security areas. Defining a solid password policy, and configuring your system to enforce the policy, greatly reduces this security risk. Requiring complex passwords that are changed regularly minimizes the likelihood of unauthorized access.

The following password settings should be considered when defining a password policy:

- Enforce password history to limit the reuse of old passwords.
- Enforce password ageing to force frequent changing of passwords.
- Enforce minimum password length to reduce the password guessing.
- Enforce password complexity requirements to further reduce password guessing.
- Make sure passwords are not stored using reversible encryption.

Remote Access

The need for access to process information, configuration information and system information from outside of the systems' domain has become a common need in all Process Systems. Well-defined policies and procedures to manage remote access to the system by other company business units and/or suppliers and vendors will greatly reduce the possibility of security threats penetrating the system.

The following ideas can be considered when dealing with remote access:

- Limit access as much as possible by defining different access levels (based on need).
- Do not allow direct access. Instead, use a proxy such as a Terminal Services (Remote Desktop) connection.
- Enforce a mandatory PC security scan of any equipment that is brought onsite. Provide written policies with repercussions for non-compliance in place for connecting foreign machines into the Control Network.
- Have separate role based user groups for temporary accounts and review this user list often.
- Define and document all outside system access routes and accounts.

Physical Access

Protecting critical process control components such as servers, routers, switches, PLCs, and controllers should be strongly considered. The assets must be protected under lock and key and designated personnel must be directly responsible for them. Most facilities have physical security plans in place.

These plans should be an integral part of an overall security program. By restricting unchecked computers and unauthorized users from accessing critical infrastructure components, a large portion of security threats can be avoided.

Backup and Recovery

A backup and recovery plan is critical to any security practice. The basic requirement of recovering from any level of failure due to a security or natural interruption of the system must be satisfied.

The following items should be considered when defining a backup and recovery plan:

- Define and document how each part of the system will, or can be backed up.
- Ensure backups are done as part of routine system maintenance, and when improvements or changes occur.
- Provide a documented procedure for making backups of all system configurations and assign that responsibility to appropriate personnel.
- Document all system software and hardware versioning and update the documentation as necessary.
- Provide a protected off-site repository for copies of all system backups.
- Document and provide escalation plans for recovery. Include processes and personnel assignments to implement the recovery.

Security Patch Implementation

Security patch management is one of the most critical concerns that have the largest impact on Microsoft Operating System based Supervisory and Control Systems.

Detailed attention and careful planning should be used when developing and documenting your procedures and policies for implementing security patches.

A detailed support plan from each automation vendor and security software vendor should be requested and reviewed to become part of any security patch management procedure or policy.

Platform Security Vulnerabilities

Many vulnerabilities in ICSs occur due to flaws, mis-configurations, or poor maintenance of their platforms, including hardware, operating systems, and ICS applications. These vulnerabilities can be eliminated or mitigated through various security controls, such as OS and application patching, physical access control, and security software (i.e., antivirus software). The tables in this section describe common platform vulnerabilities in the following four categories:

- Platform administration
- Platform hardware
- Platform software
- Platform malware protection.

Platform Administration

The following table summarizes vulnerabilities in the area of Platform Administration:

Vulnerability	Description
OS security patches are not maintained.	Out-of-date OSs contain newly discovered vulnerabilities that could be exploited. Documented procedures must be developed for maintaining security patches.
OS security patches implemented without exhaustive testing.	OS security patches deployed without testing could conflict with operation of the ICS. Documented procedures must be developed for testing new security patches.
Default configurations are used.	Using default configurations often leads to insecure and unnecessary open ports and exploitable network services running on hosts.
Critical configurations are not stored or backed up.	Procedures must be available for restoring ICS configuration settings in the event of accidental or attacker-initiated configuration changes to maintain system availability and prevent loss of data. Documented procedures must be developed for maintaining ICS configuration settings.
No password policy.	Password policies are needed to define when passwords must be used, how strong they must be, and how they must be maintained. Without a password policy, systems might not have appropriate password controls, making unauthorized access to systems more likely. Password policies must be developed as part of an ICS security program.
No password used.	Passwords must be implemented on ICS components to prevent unauthorized access. Password-related vulnerabilities include having no password for: <ul style="list-style-type: none">• System login (if the system has user accounts).• System power on (if the system has no user accounts).• System screen saver (if an ICS component is unattended over time).

Vulnerability	Description
Password disclosure.	<p>Passwords must be kept confidential to prevent unauthorized access. Examples of password disclosures include:</p> <ul style="list-style-type: none">• Posting passwords in plain sight, local to a system.• Sharing passwords to individual user accounts with work associates.• Communicating passwords to attackers through social engineering.• Sending passwords that are not encrypted through unprotected communications.
Password guessing.	<p>Poorly-chosen passwords can easily be guessed by humans or computer algorithms to gain unauthorized access. Examples include:</p> <ul style="list-style-type: none">• Passwords that have no strength requirements (e.g., length, type).• Passwords that are set to the default value as supplied by the vendor.• Passwords that are unchanged indefinitely.
Inadequate access controls applied.	<p>Poorly specified access controls can result in giving an ICS user too many or too few privileges. The following exemplify each case:</p> <ul style="list-style-type: none">• System configured with default access control settings gives an operator administrative privileges.• System improperly configured results in an operator being unable to take corrective actions in an emergency situation. <p>Access control policies must be developed as part of an ICS security program.</p>

Platform Hardware Vulnerabilities

The following table summarizes vulnerabilities in the area of Platform Hardware:

Vulnerability	Description
Inadequate physical protection for critical systems.	Access to the control center, field devices, portable devices, media, and other ICS components needs to be controlled. Many remote sites are often unstaffed and may not be physically monitored.
Non-critical personnel have physical access to equipment.	Physical access to ICS equipment should be restricted to only the necessary personnel. Improper access to ICS equipment can lead to any of the following: <ul style="list-style-type: none">• Physical theft of data and hardware.• Physical damage or destruction of data and hardware.• Unauthorized changes to the functional environment (e.g., data connections, unauthorized use of removable media, adding/removing resources).• Disconnection of physical data links.• Undetectable interception of data (keystroke and other input logging).
Insecure remote access on ICS components.	Modems and other remote access capabilities that enable control engineers and vendors to gain remote access to systems must be deployed with security controls to prevent attackers from gaining access to the ICS.
Dual network interface cards (NIC) to connect networks.	Machines with dual NICs connected to different networks could allow unauthorized access and passing of data from one network to another.
Undocumented assets.	To properly secure an ICS, there has to be an accurate listing of the assets in the system. An inaccurate representation of the control system and its components could leave an unauthorized access point or backdoor into the ICS.

Vulnerability	Description
Safety systems integrated with ICS.	Safety systems, which are designed to bring the process to a safe state in the event of a failure, are being integrated with open ICS. This level of integration introduces the risk of a single point of failure, which not only disrupts the process, but may also prevent the safety systems from responding to such disruptions.
Radio frequency pulses.	The hardware used for control systems is vulnerable to radio frequency (RF) pulses. The impact can range from temporary disruption of command and control to permanent damage to circuit boards.
Lack of backup power.	Without backup power to critical assets, a general loss of power will shut down the ICS and could create an unsafe situation.
Loss of environmental control.	Loss of environmental control could lead to processors overheating. Some processors will shut down to protect themselves, and some just melt if they overheat.

Platform Software Vulnerabilities

The following table summarizes vulnerabilities in the area of Platform Software:

Vulnerability	Description
Buffer overflow.	Software used to implement ICS could be vulnerable to buffer overflows; attackers could exploit these to perform various attacks.
Installed security capabilities not enabled by default.	Security capabilities that were installed with the product are useless if they are not enabled.
Denial of service.	Software used to implement ICS could be vulnerable to denial of service attacks, resulting in the prevention of authorized access to a system resource or the delaying of system operations and functions.
Mishandling of undefined, poorly defined, or "illegal" conditions.	Some ICS implementations are vulnerable to packets that are malformed or contain illegal or otherwise unexpected field values.

Vulnerability	Description
OPC relies on Remote Procedure Call (RPC) and Distributed Component Object Model (DCOM).	OPC is vulnerable to the known RPC/DCOM vulnerabilities.
Use of insecure industry-wide ICS protocols.	Distributed Network Protocol (DNP) 3.0, Modbus, Profibus, and other protocols are common across several industries and protocol information is freely available. These protocols often have little to no security capabilities.
Use of clear text.	Many ICS protocols transmit messages in clear text across the transmission media, making them susceptible to eavesdropping by attackers.
Availability of protocol analyzers to decode structures.	Protocol analyzers are readily available to decode structures for nearly every protocol in use today. Attackers that monitor ICS communications can use protocol analyzers to decode the data within those communications if they are not encrypted.
Use of proprietary software that has been discussed at conferences and in periodicals.	Proprietary software issues are discussed at international conferences and available through technical papers and periodicals. Also, control system maintenance manuals are available from the vendors. This information can help attackers to create successful attacks against ICSs.
Inadequate authentication and access control for configuration and programming software.	Unauthorized access to configuration and programming software could provide the ability to corrupt the device.
Intrusion detection/prevention software not installed.	Attacks can result in loss of system availability; the capture, modification, and deletion of data; and incorrect execution of control commands. IDS/IPS software can stop or prevent various types of attacks, including denial of service attacks, and also identify attacked internal hosts, such as those infected with worms.
Logs not maintained.	Without proper and accurate logs, it might be impossible to determine what caused a security event to occur.

Platform Malware Protection Vulnerabilities

The following table summarizes vulnerabilities in the area of Platform Malware Protection:

Vulnerability	Description
Malware protection software not installed.	Malicious software can result in performance degradation, loss of system availability, and the capture, modification, or deletion of data. Inadequate malware protection software, such as antivirus software, is needed to prevent systems from being infected by malicious software.
Malware protection software or definitions not current.	Outdated malware protection software and definitions leave the system open to new malware threats.
Malware protection software implemented without comprehensive testing.	Malware protection software deployed without testing could conflict with operation of the ICS.

Infrastructure Assessment

Vulnerabilities in ICSs may result from flaws, mis-configurations, or poor administration of ICS networks and their connections with other networks. These vulnerabilities can be eliminated or mitigated through various security controls, such as encrypting network communications, restricting network traffic flows, and providing physical access control for network components.

The following information describes network concerns at a high level. Detailed considerations are included after the following tables.

Vulnerabilities are summarized in the following categories, and are described next:

- Network Administration
- Network Hardware
- Network Perimeter
- Network Monitoring and Logging
- Communication
- Wireless Connection

Network Administration

Vulnerability	Description
Weak network security architecture.	The network infrastructure environment within the ICS has often been developed and modified based on business and operational requirements, with little consideration for the potential security impacts of the changes. Over time, security gaps have likely been introduced or never addressed correctly within particular portions of the infrastructure and may not have received appropriate remediation. These gaps may represent back doors into the ICS. Generally in this scenario, domain isolation has not been employed because the critical nature of the ICS or the ramifications of its failure is not well understood. Additionally inexperienced IT security personnel tend to believe that securing the business domain is more critical than securing the ICS, even though fantastic amounts of lost revenue and/or environmental damage along with possible loss-of-life scenarios routinely occur during ICS attacks or incapacity.
Data flow controls not employed.	Data flow controls such as access control lists (ACL) are needed to restrict which systems can directly access network devices. Generally, only network administrators should be able to access such devices directly, so data flow controls must ensure that other systems cannot directly access the devices.
Poorly configured IT security equipment.	Using default configurations often leads to insecure and unnecessary open ports and exploitable network services running on hosts. Improperly configured Firewall rules and router ACL can allow unnecessary traffic.
Network device configurations not stored or backed up.	Procedures must be available for restoring network device configuration settings in the event of accidental or attacker-initiated configuration changes to maintain system availability and prevent loss of data. Documented procedures must be developed for maintaining network device configuration settings.

Vulnerability	Description
Passwords are not encrypted in transit.	Passwords transmitted in clear text across transmission media are susceptible to eavesdropping by attackers, who could reuse them to gain unauthorized access to a network device. Such access could allow an attacker to disrupt ICS operations or to monitor ICS network activity.
Passwords exist indefinitely on network devices.	Passwords need to be changed regularly so that if one becomes known by an unauthorized party, the party has unauthorized access to the network device only for a short time. Such access could allow an attacker to disrupt ICS operations or to monitor ICS network activity.
Inadequate access controls applied.	Unauthorized access to network devices and administrative functions could allow a user to disrupt ICS operations or to monitor ICS network activity.

Network Hardware

Vulnerability	Description
Inadequate physical protection of network equipment.	Access to network equipment needs to be controlled to prevent damage and destruction.
Unsecured physical ports.	Unsecured unused physical universal serial bus (USB) and PS/2 ports could allow unauthorized connection of thumb drives, keystroke loggers, etc.

Vulnerability	Description
Loss of environmental control.	Loss of environmental control could lead to processors overheating. Some processors will shut down to protect themselves and some just melt if they overheat.
Non-critical personnel have access to equipment.	Physical access to network equipment should be restricted to only the necessary personnel. Improper access to network equipment can lead to any of the following: <ul style="list-style-type: none">• Physical theft of data and hardware.• Physical damage or destruction of data and hardware.• Unauthorized changes to the security environment (i.e., altering access control lists to permit attacks to enter a network).• Unauthorized interception and manipulation of network activity.• Disconnection of physical data links.

Network Perimeter

Vulnerability	Description
No security perimeter defined.	If the control network does not have a perimeter clearly defined, then it is not possible to ensure that the necessary security controls are deployed and configured properly. This can lead to unauthorized access to systems and data, as well as other problems. This is another reason that domain isolation must be deployed within an ICS enterprise-- it establishes a hard-line security perimeter.

Vulnerability	Description
Firewalls nonexistent or improperly configured.	A lack of properly configured firewalls could permit unnecessary data to pass between networks, such as control and corporate networks. This could cause several problems, including allowing attacks and malware to spread between networks, making sensitive data susceptible to monitoring/eavesdropping on the other network, and providing individuals with unauthorized access to systems.
Control networks used for non-control traffic.	Control and non-control traffic have different requirements, such as latency and reliability, so having both types of traffic on a single network makes it more difficult to configure the network so that it meets the requirements of the control traffic. For example, non-control traffic could inadvertently consume resources that control traffic needs, causing disruptions in ICS functions. This is a common issue for mixed domains not employing domain isolation.

Network Monitoring and Logging

Vulnerability	Description
Inadequate firewall and router logs.	Without proper and accurate logs, it might be impossible to determine what caused a security event to occur.
No security monitoring on the ICS network.	Without regular security monitoring, attacks might go unnoticed for a longer period of time, leading to additional damage and disruption. Regular security monitoring is also needed to identify problems with security controls, such as mis-configurations and failures.

Communication

Vulnerability	Description
Critical monitoring and control paths are not identified.	Rogue and/or unknown connections into the ICS can leave a backdoor for an attack.
Standard, well-documented communication protocols used in plain text.	Attackers that can monitor the ICS network activity can use a protocol analyzer or other utilities to decode the data transferred by protocols such as Telnet, FTP, and NFS. The use of such protocols also makes it easier for attackers to perform attacks against the ICS and manipulate ICS network activity.
Authentication of users, data or devices is substandard or nonexistent.	Many ICS protocols have no authentication at any level. Without authentication, it is possible to replay, modify, or spoof data or devices such as sensors.
Lack of integrity checking for communications.	There are no integrity checks built into most industrial protocols; attackers could manipulate communications undetected. To ensure integrity, the ICS can use lower layer protocols (e.g., IPsec) that offer data integrity protection.

Wireless Connection

Vulnerability	Description
Inadequate authentication between clients and access points.	Strong mutual authentication between wireless clients and access points is needed to ensure that clients do not connect to a rogue access point deployed by an attacker, and also to ensure that attackers do not connect to any of the ICS's wireless networks.
Inadequate data protection between clients and access points.	Sensitive data between wireless clients and access points should be protected using strong encryption to ensure that attackers cannot gain unauthorized access to the unencrypted data.

Detailed Network Component Considerations

The ICS Infrastructure (network) includes many components that support the supervisory and control system. Each component must be defined by its critical value and its vulnerability to attack. Every component should be reviewed and policies and procedures should be defined and applied. The documentation provides an audit trail and security level maintenance of each component.

Each component should also be evaluated to see if it is redundant. The resultant information can improve availability and protect against the system becoming unavailable due to a single point-of-failure.

Use appropriately-designed network architecture for integrating plant and IT networks, using a combination of routing, firewalls, and intrusion detection/prevention devices placed at strategic locations on the network.

Authenticator Types

One of the basic building blocks for security is the system component that authenticates users that want to access the system. These users could be actual operators and engineers.

However, authentication is necessary for other systems or services that run internally or externally to the Supervisory Control System. *All* known users must be accounted for. Authentication methods and procedures should be developed and implemented in order to reduce the risk of unauthorized access to critical systems or protected information.

Security Policy Enforcement Components

A critical area that needs to be fully explored is the components that will enforce security policies. These components are, but not limited to, Firewalls, Routers, Switches, and Operating System Services.

Each device or software package that is deployed for security policy enforcement should be defined by its type of enforcement, and the impact to system on failure. Any enforcement component that is defined as **critical** should be deployed in a redundant configuration if possible.

Firewalls, Routers, Switches

Firewalls, Routers, and Switches have become an integral part of all Supervisory and Control systems.

Firewalls provide for a way to isolate and control communication between network layers or segments, and between operational units. Provide a detailed inventory of communication ports, IP addresses, and protocols necessary for the Supervisory and Control system to function properly. Migrate that information into a clear use policy for the components.

By defining solid policies and procedures for firewall configuration, operation, and auditing, you will be able to lock down your communication to specific ports and IP addresses that will only allow authorized communication between systems.

Defining solid policies and procedures for Routers and Switches (configuration, operation and auditing) enables better management/definition of where access is permitted, along with better control over bandwidth utilization.

Although Firewall, router, and switches have overlapping capabilities, each device should be used for its base functionality. For example, Firewalls should control communication types, Routers should forward communication by routing protocols along a proper route, and Switches should manage bandwidth by controlling communication flow between ports, and avoiding packet collisions.

Domain Controllers

Using services such as Microsoft Active Directory can provide efficient management and enforcement of access security for users, groups, and organization units. This is especially true where large numbers must be managed.

Remember that not all software includes fully-integrated, Domain-level security functionality. That software will then require local PC or package-level security implementation.

Physical Networks

The physical network is the structure on which the control system operates, and requires special attention to the design, selection of media, and installation. Complete a thorough review of any installed network segment before extending or adding components. Ensure redundant paths and proper distances are observed in order to avoid slow and unreliable communication.

All networks should be reviewed for live unsecured ports and exposed segments that could be tapped. With the complete network layout documented, recovery plans can be defined to improve system availability in the case of an incident that takes down part of the network.

Note Using network tools that scan the entire enterprise for vulnerabilities (such as tools based on the DOD (Department of Defense) database of computer vulnerabilities) can greatly facilitate this review of the physical network.

Remote Access Devices

One set of devices that should not be overlooked are Modems. Policies and procedures should be developed to control the installation and use of modems for remote access. A very good alternative to allowing modem access is to implement Virtual Private Network (VPN) access.

If a modem has to be used for remote access, a good rule is to require dial-back connections or an audit through an independent appliance such as the company PABX. Modems should never have unsupervised independent external connectivity.

Wireless Access

Wireless technologies are quickly becoming part of Supervisory and Control Systems. Wireless security includes many underlying topics that should be discussed in a planning context.

The following topics should be taken into consideration when defining a wireless implementation:

- Limit access to restricted areas by using directional antennas.
- Utilize more than the industry-standard Wired Equivalent Privacy (WEP) protocol.
- Use Virtual Private Networking (VPN) technology for client access, but remember that a VPN server can become a bottleneck.
- Use IP Security (IPSec) for computer-to-computer communication.
- Use a security solution based on 802.1X, Extensible Authentication Protocol (EAP), and Wi-Fi encryption.
- Review implementation guides from the Wireless device and the Operating System vendors.

Software

The final area of consideration when building a secure system is software. This includes existing and future installations that enable the manufacturing system. A software review enables completing a system deployment plan and a change management process that ensures the system is both continuously secure and available to its users.

The software components of a supervisory and control system can have a large impact on the security integrity of the system. When reviewing the software's security features, they must be evaluated as an integrated part of the complete system.

All software components should leverage the capabilities of the infrastructure and support configurations that meet the policies and procedures defined as necessary for system security. By reviewing all software from a security standpoint, policies and procedures can be established and augmented to audit the system and maintain high security levels.

Intrusion Protection and Prevention

Intrusion protection and prevention has become a viable way of increasing security levels within a TCP/IP LAN or WAN infrastructure. Intrusion Detection Systems monitor network traffic and alert the user/system when known malicious traffic or repeated password guessing is detected, and are used commonly by IT departments.

Intrusion Prevention technology has become the preferred system to not only detect and alert when hacking or virus/worm attacks are present, but to block such attempts by managing firewall policy, Switch ports, Router paths, and trapping e-mails before damage can be done.

However, the implementation of an Intrusion detection or Prevention system on a Supervisory and Control network does have risk.

Listed below are some considerations that must be taken into account when evaluating the use of these technologies:

- Does the system provide centralized reporting and management?
- Does the system provide multiple ways to deliver alerts?
- What level of signature-based identification of malicious or anomalous traffic is supported?
- Is connection Flood (denial of service) controls supported?
- Does the system support Alert-only mode for tuning?
- Does the system support the software and applications already installed or about to be installed?
- Does the system allow creation of your own policies?
- What bandwidth and connections are supported?

Because Intrusion detection and prevention system can present a risk to functionality and operation of a Supervisory and Control System, a well-developed design with strong policies and procedures should accompany any implementation plan.

Operating Systems

The base operating system hosting all Supervisory and Control applications should be reviewed for proper deployment, configuration, and security patches.

A complete review of installed components and configured users should be the initial focus. However, Microsoft provides detailed guidance for locking down your operating systems so that security threats can be managed and eliminated. By defining what Supervisory and Control software is to be deployed to a system, you can define the level of lock-down, and at the same time allow for full functionality of manufacturing applications.

Databases

Databases and Relational Database Management Systems (RDBMSs) such as Microsoft SQL Server have become a common component of all manufacturing systems.

With the need to allow database access, and the need to update and append the database, you must be very deliberate in the approach that is taken when locking down a database.

A set of security procedures that define standard configuration and access to databases can be compiled by mapping users (people and services) that need access to the data, and by defining usable database security policies.

Information portals or proxies should be designed into the system and implemented. End users should never have direct access to production servers.

Other Manufacturing Systems Components

Many other software components make up a complete Manufacturing System:

- Batch Management
- Work in Progress
- Enterprise Resource Planning
- Maintenance Management

Each of these systems can present many security risks. Making sure that the integration of expert systems and the access need by these systems to the control system is well documented.

This enables policies/procedures development that ensures you maintain the lowest security risk possible. The other important aspect of expert systems that are part of your manufacturing environment, is that many different operating systems, protocols, clients, and users must be supported. By defining a layered approach to implementing security, each system can be placed at the proper level that will allow for the correct access level to, and interaction with, the supervisory and control system.

Security Threats and Attack Scenarios

Threats to control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, malicious intruders, complexities, accidents, and natural disasters.

To protect against these threats, it is necessary to create a secure cyber-barrier around the ICS. However, ICSs are also at risk of being attacked by insiders. Such an attack could come from a malicious action or an accidental action that results in damage.

The following table summarizes the possible threats:

Threat	Description
Bot-network operators	Bot-network operators are hackers; however, instead of breaking into systems for the challenge or bragging rights, they take over multiple systems in order to coordinate attacks and to distribute phishing schemes, spam, rootkit, and malware attacks. The services of these networks are sometimes made available on underground markets (e.g., purchasing a denial-of-service attack, servers to relay spam or phishing attacks, etc.).
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized crime groups use spam, phishing, and spyware/malware to commit identity theft and online fraud. International corporate spies and organized crime organizations also pose a threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information-gathering and espionage activities. Additionally, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power - impacts that could affect the daily lives of U.S. citizens across the country.

Threat	Description
Hackers	Hackers break into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency, the large majority of hackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.
Insiders	The disgruntled organization insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors as well as employees who accidentally introduce malware into systems.
Phishers	Individuals, or small groups, that execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware/malware to accomplish their objectives.
Spammers	Individuals or organizations that distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations (i.e., denial of service).

Threat	Description
Spyware/malware authors	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware, and most recently rootkits. Several destructive computer viruses and worms have recently harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster. Current technologies include self-tunneling Port Scanners, fully capable of reporting the information back through a "secure" business domain to machines having Internet access, and rootkit poisoned operating system files which contain malicious code but look and act like normal OS files and services.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

ICS Attack Scenarios

There are many possible scenarios for inflicting damage to an ICS system. Entities or individuals with malicious intent might take one or more of the following actions to successfully attack control systems:

- Disrupt the operation of control systems by delaying or blocking the flow of information through control networks, thereby denying availability of the networks to control system operators.
- Make unauthorized changes to programmed instructions in PLCs, RTUs, DCS, or SCADA controllers, change alarm thresholds, or issue unauthorized commands to control equipment, which could potentially result in damage to equipment (if tolerances are exceeded), premature shutdown of processes (such as prematurely shutting down transmission lines), or even disabling of control equipment.
- Send false information to Control System operators either to disguise unauthorized changes or to initiate inappropriate actions by system operators.
- Modify the control system software or configuration settings, producing unpredictable results.
- Interfere with the operation of safety systems.

- Introduce malicious software (e.g., virus, worm, Trojan horse) into the system.

In control systems that cover a wide geographic area, the remote sites are often unstaffed and may not be physically monitored. If such remote systems are physically breached, the attackers could establish a connection back to the control network.

The following are two possible ICS attack scenarios:

- Using war dialers (simple personal computer programs that dial consecutive phone numbers looking for modems) an attacker finds modems connected to the programmable circuit breakers of the electric power control system, cracks passwords that control access to the circuit breakers, and changes the control settings to cause local power outages and damage equipment. The attacker lowers the settings from 500 Ampere (A) to 200 A on some circuit breakers, taking those lines out of service and diverting power to neighboring lines. At the same time, the attacker raises the settings on neighboring lines to 900 A, preventing the circuit breakers from tripping and overloading the lines. This causes significant damage to transformers and other critical equipment, resulting in lengthy repair outages.
- A power plant serving a large metropolitan district has successfully isolated the control system from the business network of the plant, installed state-of-the-art firewalls, and implemented intrusion detection and prevention technology. An engineer innocently downloads information on a continuing education seminar at a local college, inadvertently introducing a virus into the control network. Just before the morning peak, the operator screens go blank and the system is shut down.

Although these scenarios are hypothetical, they represent the kinds of real threats facing control systems. The following section provides summaries of several real ICS incidents.

Attack Event Documentation

An accurate accounting of cyber attacks on control systems is difficult to determine. However, those in the ICS industry who have been focusing on this space see similar growth trends between vulnerabilities exposed in traditional IT systems and those being found in control systems.

The British Columbia Institute of Technology (BCIT) maintains an [Industrial Security Incident Database \(ISID\)](#), designed to track incidents of a cyber security nature that directly affect industrial control systems and processes. This includes events such as accidental cyber-related incidents, as well as deliberate events such as unauthorized remote access, denial of service attacks, and virus/worm infiltrations.

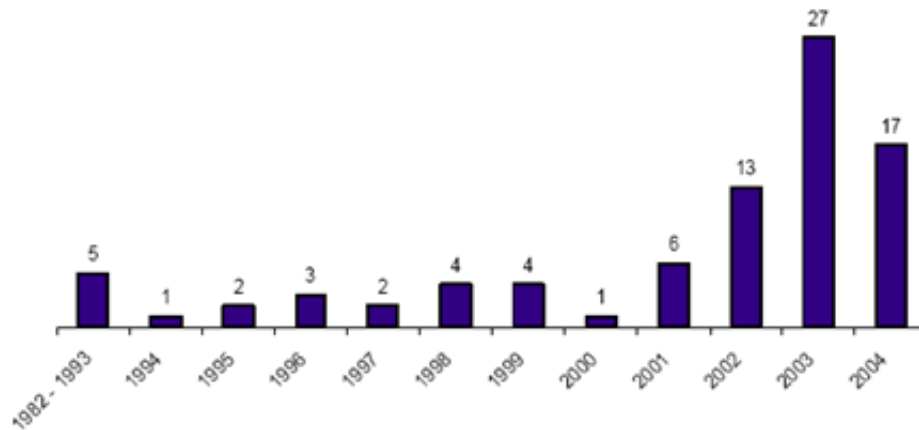
Data is collected through research into publicly-known incidents and from private reporting by member companies that wish to have access to the database. Each incident is investigated and then rated according to reliability (confirmed, likely but unconfirmed, unlikely or unknown, and hoax/urban legend).

The collected data includes the following items:

- Incident Title
- Incident Date
- Report Reliability
- Incident Type (e.g., accident, virus)
- Industry (e.g., petroleum, automotive)
- Entry Point (e.g., Internet, wireless, modem)
- Perpetrator
- System Type and Impacted Hardware
- Brief Description
- Impact on Company
- Measures to Prevent Recurrence
- References.

As of June 2004, 94 incidents had been investigated and logged in the database, with 22 incidents still pending investigation. Of these, 8 were flagged as hoax/urban legend and removed from the study data.

The following figure shows the trend of events between 1982 and 2004, which shows a sharp increase in events starting around 2001. After 2001, incidents changed from being mostly internal and accidental, to external:



Attack Event Categories and Descriptions

The complexity of modern ICSs leaves many vulnerabilities as well as vectors for attack. Attacks can come from the business network, or directly via the Internet, virtual private networks, wireless networks, and dial-up modems:

Attack Event Categories

Three broad categories have been identified in order to classify ICS attack events:

- Intentional targeted attacks such as gaining unauthorized access to files, performing a denial of service, or spoofing e-mails (i.e., forging the sender's identity for an email).
- Unintentional consequences or collateral damage from worms and viruses.
- Unintentional internal security breaches, such as inappropriate testing procedures of operational systems or inadequate control systems architecture.

Of the three, targeted attacks are the least frequent. Targeted attacks are potentially the most damaging, but also require detailed knowledge of the entity and supporting infrastructure. Consequently, the most likely attacker is a disgruntled employee, ex-employee, or someone else who has worked with or for the entity being attacked.

Attack Event Descriptions

Control Systems experts have verified numerous incidents that have affected control systems. Reported attacks include the following:

- **Salt River Project:** In 1994, the computer system of the Salt River Project (SRP), a major water and electricity provider in Phoenix, Arizona, was breached. The attacker accessed a computer or computers belonging to the SRP via a dial-up modem on a backup computer. The attacker was then able to access data and delete files on systems responsible for the monitoring and delivery of water and power to SRP customers, as well as customer, financial, and personnel records.
- **Worcester Air Traffic Communications:** In March 1997, a teenager in Worcester, Massachusetts, disabled part of the public switching network using a dial-up modem connected to the system. This knocked out phone service at the control tower, airport security, the airport fire department, the weather service, and carriers that use the airport. The tower's main radio transmitter and another transmitter that activates runway lights were shut down, as well as a printer that controllers use to monitor flight progress. The attack also knocked out phone service to 600 homes in the nearby town of Rutland.

- **Maroochy Shire Sewage Spill:** In the spring of 2000, a former employee of an Australian company that develops manufacturing software applied for a job with the local government, but was rejected. Over a 2-month period, the disgruntled rejected employee reportedly used a radio transmitter on as many as 46 occasions to remotely break into the controls of a sewage treatment system. He altered electronic data for particular sewerage pumping stations and caused malfunctions in their operations, ultimately releasing about 264,000 gallons of raw sewage into nearby rivers and parks.
- **CSX Train Signaling System:** In August 2003, the Sobig computer virus was blamed for shutting down train signaling systems throughout the east coast of the U.S. The virus infected the computer system at CSX Corp.'s Jacksonville, Florida headquarters, shutting down signaling, dispatching, and other systems. According to Amtrak spokesman Dan Stessel, ten Amtrak trains were affected in the morning. Trains between Pittsburgh and Florence, South Carolina were halted because of dark signals, and one regional Amtrak train from Richmond, Virginia to Washington and New York was delayed for more than two hours. Long-distance trains were delayed between four and six hours.
- **Davis-Besse:** In August 2003, the Nuclear Regulatory Commission confirmed that in January 2003, the Microsoft SQL Server worm known as Slammer infected a private computer network at the idled Davis-Besse nuclear power plant in Oak Harbor, Ohio, disabling a safety monitoring system for nearly 5 hours. The plant's process computer failed, and it took about 6 hours for it to become available again. Slammer reportedly also affected communications on the control networks of at least five other utilities by propagating so quickly that control system traffic was blocked.
- **USSR Natural Gas Pipeline:** In his book "At the Abyss" (Ballantine, 2004, ISBN 0-89141-821-0), Thomas C. Reed, Ronald Reagan's Secretary of the Air Force, described how the United States arranged for the Soviets to receive intentionally flawed process control software for use in conjunction with the USSR's natural gas pipelines, which were to generate critically needed hard currency for the USSR. Reed stated that "the pipeline software that was to run the pumps, turbines, and valves was programmed to go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds." The result was a three-kiloton blast in a remote area of Siberia in 1982, which fortunately did not result in any deaths. This was the most monumental non-nuclear explosion and fire ever seen from space.
- **Zotob Worm:** In August 2005, a round of Internet worm infections knocked 13 of DaimlerChrysler's U.S. automobile manufacturing plants offline for almost an hour, stranding workers as infected Microsoft Windows systems were patched. Plants in Illinois, Indiana, Wisconsin, Ohio, Delaware, and Michigan were knocked offline. While the worm affected primarily Windows 2000 systems, it also affected some early versions of Windows XP. Symptoms include the repeated shutdown and rebooting of a computer. Zotob and its variations caused computer outages at heavy-equipment maker Caterpillar Inc., aircraft-maker Boeing, and several large U.S. news organizations.

Detecting and Preventing Insider Threats

Insiders have a significant advantage over others who might want to cause harm to an organization. Insiders are aware of the policies, procedures, and technology used in their organizations, and they may also be aware of system vulnerabilities, such as loosely-enforced policies and procedures, or exploitable technical flaws in networks or systems.

Insiders can bypass physical and technical security measures designed to prevent unauthorized access from outside sources. For example, firewalls, intrusion detection systems, and electronic building access systems are implemented primarily to defend against external cyber threats.

The threat of attack from insiders is real and substantial. The 2004 ECrime Watch Survey conducted by the United States Secret Service, CERT® Coordination Center (CERT/CC), and CSO Magazine, found that in cases where respondents could identify the perpetrator of an electronic crime, 29 percent were committed by insiders.

The impact from insider attacks can be devastating. One complex case of financial fraud committed by an insider in a financial institution resulted in losses of over \$600 million. Another case involving a logic bomb written by a technical employee working for a defense contractor resulted in \$10 million in losses and the layoff of 80 employees.

Note A "logic bomb" is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files, should he ever leave the company (and the salary database).

Carnegie Mellon University conducts a variety of research projects on insider threats. One of the conclusions reached is that insider attacks have occurred across all organizational sectors, causing significant damage to the affected organizations. These acts have ranged from "lowtech" attacks, such as fraud or theft of proprietary information, to technically sophisticated crimes that sabotage the organization.

Damages are not only financial but can also include severe damage to the organization's reputation, resulting from widespread public reporting of the event.

CERT/CC is conducting the Insider Threat Study (in partnership with the United States Secret Service) to gather extensive insider threat data from more than 150 case files of crimes that involve most of the nation's critical infrastructure sectors.

This study shows that use of the widely accepted best practices for information security could have prevented many of the insider attacks examined. Part of the research of insider threat cases entailed an examination of how each organization could have prevented the attack, or at the very least detected it earlier.

Rather than requiring new practices or technologies for prevention of insider threats, the research instead identifies existing best practices that are critical to the mitigation of the risks from malicious insiders.

Best Practices for Stopping Insider Attacks

Insiders can be stopped, but stopping them is a complex task. Insider attacks can only be prevented through a layered defense strategy consisting of policies, procedures, and technical controls. Therefore, management must pay close attention to many aspects of its organization, including its business policies and procedures, organizational culture, and technical environment.

They must look beyond information technology to the organization's overall business processes and the interplay between those processes and the technologies used.

Best Practice Summary

Implementing the following "best practices" to prevent insider attacks provides an organization with defensive measures that can prevent, or detect many insider attacks before they occur.

The practices are summarized in the following section and include links to their detailed content. Case studies are included with the detailed information as examples.

- ["Institute Periodic Employee Security Awareness Training" on page 75:](#)

The first line of defense from insider threats is employees. A culture of security awareness must be instilled in the organization so that all employees understand the need for policies, procedures, and technical controls. All employees in an organization must understand that security policies and procedures exist, that there is a good reason for why they exist, that they must be enforced, and that there can be serious consequences for infractions.

- ["Enforce Separation of Duties and Least Privilege" on page 77:](#)

When all employees are adequately trained in security awareness, and responsibility for critical functions is divided among employees within the organization, the possibility that an individual will commit fraud or sabotage without the cooperation of another individual is limited. Effective separation of duties requires the implementation of "least privilege," that is, authorizing people only for the resources they need to do their jobs.

- ["Implement Strict Password and Account Management Policies and Practices" on page 79:](#)

If the organization's computer accounts can be compromised, insiders have an opportunity to circumvent both manual and automated mechanisms that exist to prevent insider attacks.

- ["Log, Monitor, and Audit Employee Online Actions" on page 81:](#)

When account and password policies and procedures are in place and enforced, the organization can associate online actions with the employee who performed them. Logging, periodic monitoring, and auditing provide the opportunity to discover and investigate suspicious insider actions before more serious events occur.

- ["Use Extra Caution with System Administrators and Privileged Users" on page 82:](#)

Logging and monitoring is performed by a combination of system administrators and privileged users. Therefore, additional vigilance must be devoted to those users.
- ["Actively Defend Against Malicious Code" on page 84:](#)

Logic bombs or installation of other malicious code on the system or network is executed by system administrators or privileged users. These attacks are stealthy and therefore difficult to detect ahead of time, but effective practices can be implemented for early detection.
- ["Use Layered Defense Against Remote Attacks" on page 86:](#)

When employees are trained and vigilant, accounts are protected from compromise, and employees know that their actions are being logged and monitored, disgruntled insiders think twice about attacking systems or networks at work. Insiders tend to feel more confident and less inhibited when they have little fear of scrutiny by coworkers; therefore, remote access policies and procedures must be carefully designed and implemented.
- ["Monitor and Respond to Suspicious or Disruptive Behavior" on page 88:](#)

Organizations must closely monitor other suspicious or disruptive behavior in the workplace. Policies and procedures should be in place for employees to report such behavior when they observe it in coworkers, with required follow-up by management.
- ["Deactivate Computer Access Following Termination" on page 90:](#)

When an employee terminates employment, whether the circumstances were favorable or not, the organization must initiate a rigorous termination procedure that disables all the employee's access points to the organization's networks, systems, applications, and data.
- ["Collect and Save Data for Use in Investigations" on page 92:](#)

Should an insider attack, it is important that the organization have evidence in hand to identify the insider and prosecute them.
- ["Implement Secure Backup and Recovery Processes" on page 93:](#)

Despite the precautions implemented by an organization, an insider attack is still possible. Therefore, the organization must prepare for that possibility by implementing secure backup and recovery processes that are tested periodically.
- ["Clearly Document Insider Threat Controls" on page 95:](#)

As the organization acts to mitigate insider threat, clear documentation ensures fewer gaps exist for attack, provides better employee comprehension, and fewer misconceptions that the organization is acting in a discriminatory manner.

Institute Periodic Employee Security Awareness Training

Without broad understanding and buy-in from the organization, any technical or managerial controls are short-lived.

Employees and managers need to understand that there is no "profile" of a malicious insider.

Reported cases involve both highly technical people and those who have very minimal understanding of the systems they exploited. Perpetrators ages range from late teens to retirement age. Both men and women can be malicious insiders.

These people are introverted "loners," aggressive "get it done" people, and extroverted "star players." Their positions include low-wage data entry clerks, cashiers, programmers, artists, system and network administrators, salespersons, managers, and executives. They are new hires, long-term employees, currently employed, recently terminated employees, contractors, and temporary employees.

Security awareness training must encourage employees to identify malicious insiders by behavior, not by stereotypical characteristics. Behaviors of concern include making threats against the organization, bragging about the damage one could do to the organization, or discussing plans to work against the organization. Attempts to gain other employees' passwords and to fraudulently obtain access through trickery or exploitation of a trusted relationship must be reported.

Organizations must provide training programs that create a culture of security that is appropriate for them and one that includes both security and non-security personnel. For effectiveness and longevity, the security measures must be tied to the organization's mission, values, and critical assets.

For example, when the organization places a high value on quality customer service, it may view security as protection of individual customer information, as well as the ability to serve customers. That organization could train its members about malicious employee actions focusing on a number of key issues, including the following:

- Reducing risks to customer information by auditing access to customer records (page 81).
- Requiring separation of duties between employees who modify customer accounts and those who approve modifications or issue payments (page 77).
- Using secure backup and recovery methods to ensure availability of customer service data (page 93).

Training on reducing risks to customer service processes would focus on the following strategies:

- Protecting computer accounts used in these processes (page 79).
- Using malicious code detection tools (page 84).
- Detecting and reporting disruptive behavior by employees (page 88).

- Implementing proper system administration safeguards for critical servers (page 82, page 86, and page 90).

Training content would be based on documented policy (page 95), including a confidential means of reporting security issues with appropriate follow-up to security reports.

Employees must understand that the organization has policies and procedures in place, and that the organization will respond to detected security issues in a fair and prompt manner.

Separation of duties and remote access monitoring should be explained. While employee alertness is key to detecting many insider attacks, several cases have been detected because of abnormal system activity (including download of sensitive material to home computers, unusual system load, changes in system configuration, and illicitly escalated user privilege). Employees should be notified that system activity is monitored, especially system administration and privileged activity.

All employees should be trained in their personal responsibility, such as protection of their own passwords and work products.

Case Studies

Case Study

The lead developer of a critical application used by his organization had extensive control over the source code for that application. He made sure that the only copy of the source code was on his company-provided laptop; no backups were performed, and very little documentation existed, although management had repeatedly requested documentation for the system.

The insider told his coworkers he had no intention of documenting the source code and any documentation he did write would be encrypted. He also stated that he thought poorly of his management because they had not instructed him to make backup copies of the source code.

A month after learning of a pending demotion, he erased the hard drive of his laptop and then quit his job the next day. His actions deleted the only copy of the source code the organization possessed. It took more than two months to recover the source code from the insider—and that was only after it was located in encrypted form at his home in a search conducted by law enforcement officials.

Another four months elapsed before the insider provided the password to decrypt the source code. During this time the organization was forced to rely on the executable version of the application, and had no ability to make any modifications.

This case illustrates the importance of security awareness training for all employees. If the insider's team members had been informed that the security and survivability of the system was their responsibility and they had been presented with a clear procedure for reporting behavior that concerned them, then they might have notified management of the insider's statements and actions in time for management to prevent the attack.

Case Study

Another insider case illustrates a much less technically sophisticated attack, but one that could have been avoided or successfully prosecuted if proper policies and training had been in place:

Four executives of a national computer and network support services consulting firm left to form a competing company. A few days before they left, one of the insiders ordered a backup copy of the hard drive on his work computer from the Internet service the company used to back up its data. The hard drive contained customer lists and other sensitive information. The company alleged that its consulting services agreement and price list were sent by email from the insider's work computer to an external email account registered under his name.

The insiders, two of whom had signed confidentiality agreements with the original employer, disputed the fact that the information they took was proprietary, saying that it had been published previously. Clear policies regarding definition of proprietary information and rules of use could have prevented the attack or provided a clearer avenue for prosecution.

Enforce Separation of Duties and Least Privilege

While security awareness training is an excellent start, basic controls for separation of duties and least privilege must be in place to limit the damage that malicious insiders can inflict.

Separation of duties requires dividing of functions among people within an organization, in order to limit the possibility that one individual could commit fraud or sabotage without the cooperation of another employee. A particular separation of duties type called **twoperson rule** is often used in cases where two people must participate in a task for it to be executed successfully.

Examples include requiring two bank officials to sign large cashier's checks, or requiring verification and validation of source code before the code is released operationally. In general, employees are less likely to engage in malicious acts if they must collaborate with another employee.

Effective separation of duties requires the implementation of least privilege, that is, authorizing people only for the resources they need to do their job. Organizations define a work role for each employee, which characterizes their job responsibilities and the access (to organizational resources) necessary to fulfill those responsibilities. Insider risk can be greatly mitigated by defining and separating the roles responsible for key business processes and functions.

For example:

- Online management authorization can be required for critical data entry transactions.
- Code reviews can be instituted for the software development and maintenance process.
- Configuration management processes and technology can be used to control software distributions and system modification.

- Auditing procedures can be designed to ensure that collusion between employees is avoided.

Physical, administrative, or technical controls can be used to restrict employees' access to only those resources needed to accomplish their jobs.

Access control based on separation of duties, and least privilege practices are crucial to mitigating the risk of insider attack. These principles have implications in both the physical and the virtual worlds.

In the physical world, organizations must prevent employees from gaining physical access to resources not required by their work roles. For example, chemical researchers must have access to their laboratory spaces but do not need access to human resources file cabinets. Likewise, human resources personnel must access personnel records, but do not need access to laboratory facilities.

In the virtual world, organizations must prevent employees from gaining online access to information or services that are not required by their work roles.

This kind of control is often called Role Based Access Control. Role Based Access Control is a way of controlling access based on the context of the requestor and the relationship to the data in question. The context is the role of the requester, both from a business perspective and the technical—for example, a system manager that is a business role and has technical access to make changes to the running application. Requestors are organized into groups and policies are created that apply to those groups.

Prohibiting access of personnel in one role from the functions permitted by another role limits the damage they can inflict if they become disgruntled or otherwise decide to exploit the organization for their own purposes.

Case Study

A currency trader (who also happened to have a college minor in computer science) developed much of the software used by his organization to record, manage, confirm, and audit trades. He implemented obscure functionality in the software that enabled him to conceal his illegal trades. Over time, he evolved the software to facilitate different methods of hiding his activities in order to reduce the risk of detection. In this case, it was nearly impossible for auditors to detect his activities.

The insider, who consented to be interviewed for the Insider Threat Study, told the study researchers that problems can arise when the fox is guarding the henhouse."

The insider's supervisor managed both the insider and the auditing department responsible for ensuring his trades were legal or compliant. When auditing department personnel raised concern about the insider's activities, they were doing so to the insider's supervisor (who happened to be their supervisor as well). The supervisor directed auditing department personnel not to worry about the insider's activities and to cease raising concern, for fear the insider would become frustrated and quit.

This case illustrates two ways in which separation of duties can prevent an insider attack or detect it earlier:

- End-users of an organization's critical systems should not be authorized to modify system functionality or access the underlying data.
- Responsibility for critical data, and responsibility for auditing that critical data should never be assigned to the same person.

Case Study

A supervisor fraudulently altered U.S. immigration asylum decisions using his organization's computer system in return for payments of up to several thousand dollars per case, accumulating \$50,000 over a two-year period.

The insider would approve an asylum decision himself, request that one of his subordinates approve the decision, or overturn someone else's denial of an asylum application.

Several foreign nationals either admitted in an interview or pleaded guilty in a court of law to lying on their asylum applications and bribing public officials to get approval of their applications.

The organization had implemented separation of duties via role based access control by limiting authorization for approving or modifying asylum decisions to supervisors' computer accounts. However, supervisors were able to alter any decisions in the entire database, not just those assigned to their subordinates.

An additional layer of defense, least privilege, also could have been implemented to prevent supervisors from approving asylum applications or overturning asylum decisions with which they were not involved.

Implement Strict Password and Account Management Policies and Practices

If the organization's computer accounts can be compromised, insiders have an opportunity to circumvent mechanisms that are in place to prevent insider attacks. Therefore, computer account and password management policies and practices are critical to impede an insider's ability to sabotage the organization's systems.

Fine-grained access control combined with proper computer account management ensures that:

- Access to all of the organization's critical electronic assets is controlled so that unauthorized access is not possible.
- System Access is logged and monitored so that suspicious access can be detected and investigated.
- System Access can be traced from the computer account to the individual associated with that account.

Password policies and procedures should ensure that all passwords are strong, employees do not share their passwords with anyone, employees change their passwords periodically, and all computers execute password-protected screen savers. As a result, all activity from any account should be attributable to its owner.

Employees should also report all attempts at account compromises rather than permit a compromise to happen due to ignorance of potential consequences or lack of a reporting mechanism.

Periodic account audits, combined with technical controls, enable identification of the following security risks:

- Backdoor accounts that could be used later for malicious actions by an insider, whether those accounts were specifically set up by the insider or were left over from a previous employee.
- Shared accounts whose password was known by the insider and not changed after that person's termination.

Every user account should be evaluated periodically. Limiting accounts to those that are absolutely necessary, with strict procedures and technical controls (so that all online activity by those accounts can be traced directly to an individual user), diminishes an insider's ability to conduct anonymous malicious activity.

Account management policies (including documentation of all access privileges for all users) enable a straightforward termination procedure that reduces the risk of attack by terminated employees.

Case Study

A disgruntled software developer downloaded the password file from his organization's UNIX server to his desktop. Next, he downloaded a password cracker from the Internet and proceeded to "break" approximately 40 other passwords, including the root password.

Fortunately, he did no damage, but he did access parts of the organization's network for which he was not authorized.

The insider was discovered when he bragged to the system administrator that he knew his root password. As a result, his organization modified its policies and procedures to implement countermeasures to prevent such attacks in the future. System administrators were permitted to run password crackers and notify users with weak passwords, and it improved security training for employees on how and why to choose strong passwords.

Case Study

A second case also illustrates the importance of employee awareness of password security:

Two temporary data entry clerks and one permanent employee were able to embezzle almost \$70,000 from their company by fraudulently using other employees' computer accounts. The system's role based access provided the other employees' accounts with access to privileged system functions.

The clerks used those accounts without authorization to subvert the business process governing vendor payment. First, they entered valid data into the database using their own accounts. Then they used the other, unauthorized accounts to modify the vendor's name and address to that of a friend or relative, issued the check from the system, and then modified the data back to the original, valid vendor information.

The fraud was discovered after almost five months when an accountant in the general ledger department noticed that the number of checks issued was larger than normal, and further investigation revealed the irregularities in the handling of the checks.

Log, Monitor, and Audit Employee Online Actions

Logging, monitoring, and auditing can lead to early discovery and investigation of suspicious insider actions.

When account and password policies and procedures are in place and enforced, an organization can associate online actions with the employee who performed them.

Logging, monitoring, and auditing provide an organization with the opportunity to discover and investigate suspicious insider actions before serious events occur.

In the technical security domain, "auditing" refers to examination and verification of various network, system, and application logs. To prevent or detect insider threats, it is important that auditing involve the review and verification of all of the [organization's critical assets](#).

Furthermore, auditing must examine and verify integrity as well as the legitimacy of logged access.

Automated integrity checking should be considered for flagging suspicious transactions that do not adhere to predefined business rules for manual review. Insider threats are most often detected by a combination of automated logging and manual monitoring or auditing.

For example, integrity checking of computer account creation logs involves automated logging combined with manual verification that every new account has been associated with a legitimate system user and that the user is aware of the account's existence. Likewise, data audits typically involve manual processes, such as comparing electronic data modification history to paper records or examining electronic records for suspicious discrepancies.

Auditing should be both ongoing and random. If employees are aware that monitoring and auditing is a regular, ongoing process and that it is a high priority for the individuals who are responsible for it, it can serve as a deterrent to insider threats. For example, if a disgruntled system administrator is aware that all new computer accounts are reviewed frequently, then it is less likely that they will create backdoor accounts for later malicious use.

On the other hand, it probably is not practical to institute daily monitoring of every financial transaction in a financial institution. Monthly and quarterly auditing provides one layer of defense against insiders, but it also provides a predictable cycle on which insiders could design a fraud scheme that could go undetected over a long period of time.

Random auditing of all transactions for a given employee, for example, could add just enough unpredictability to the process to deter an insider from launching a contemplated attack.

Case Study

While performing remote access monitoring, a large international company noticed that a former consultant had obtained unauthorized access to its network and created an administrator account.

This prompted an investigation of the former insider's previous online activity. The investigation revealed that he had run several different password-cracking programs on the company's network five different times over a ten-month period. Initially, he stored the cracked passwords in a file on the company's server. He later installed a more sophisticated password cracking program on the company's system. This program enabled him to automatically transfer all accounts and passwords that could be cracked to a remote computer on a periodic basis. Five thousand passwords for company employees were successfully transferred.

This case illustrates the importance of logging and proactive monitoring. Because of those practices, this insider's actions were detected before any malicious activity was committed using the accounts and passwords or the backdoor account.

Case Study

Another case study provides a contrasting example—one in which *lack* of auditing permitted the insider to conduct an attack that was less technically sophisticated but that enabled him to steal almost \$260,000 from his employer over a two-year period:

The insider was the manager of a warehouse. The attack proceeded as follows:

The insider convinced his supervisor that he needed privileged access to the entire purchasing system for the warehouse. Next, he added a fake vendor to the list of authorized suppliers for the warehouse. Over the next two years, he entered 78 purchase orders for the fake vendor, and, although no supplies were ever received, he also authorized payment to the vendor.

The insider was aware of approval procedures, and all of his fraudulent purchases fell beneath the threshold for independent approval. The bank account for the vendor happened to be owned by the insider's wife.

The fraud was accidentally detected by a finance clerk who noticed irregularities in the paperwork accompanying one of the purchase orders. This fraud could have been detected earlier by closer monitoring of online activities by privileged users, particularly since this particular user possessed unusually extensive privileged access. In addition, normal auditing procedures could have validated the new vendor, and automated integrity checking could have detected discrepancies between the warehouse inventory and purchasing records.

Use Extra Caution with System Administrators and Privileged Users

System administrators and privileged users have the technical ability, access, and oversight responsibility to commit and conceal malicious activity.

System administrators and privileged users (by definition) have a higher system, network, or application access level than other users. This higher access level comes with higher risk due to the following:

- They have the technical ability and access to perform actions that ordinary users cannot.

- They can usually conceal their actions, since their privileged access typically provides them the ability to log in as other users, to modify system log files, or to falsify audit logs and monitoring reports.

Security techniques that promote "non-repudiation of action" ensure that online actions taken by users, including system administrators and privileged users, can be attributed to the person that performed them.

Note In general, non-repudiation is the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document, or the sending of a message that they originated or executed.

In the computer world and on the Internet, the now popular digital signature is used not only to ensure that a message or document has been electronically signed by the person that purported to sign the document, but also, since a digital signature can only be created by one person, to ensure that a person cannot later deny that they furnished the signature.

Therefore, if malicious insider activity occurs, non-repudiation techniques allow that activity to be attributed to a single employee. Policies, practices, and technologies exist for configuring systems and networks to facilitate non-repudiation.

However, keep in mind that system administrators and other privileged users are the people responsible for designing, creating, and implementing those policies, practices, and technologies. Therefore, separation of duties is also very important: Network, system, and application security designs should be created, implemented, and enforced by multiple privileged users.

Even when online actions can be traced to the person who engaged in the action, it is unreasonable to expect that all user actions can be monitored proactively. Therefore, while the practices discussed above ensure identification of users following detection of suspicious activity, additional steps must be taken by organizations to defend against malicious actions before they occur.

For instance, system administrators and privileged users have access to all information within their domains. Technologies such as encryption can be implemented to prevent such users from reading or modifying sensitive files to which they should not have access.

Policies, procedures, and technical controls should enforce separation of duties and require actions by multiple users for all modifications to critical systems, networks, applications, and data. In other words, no single user should be permitted or be technically able to release changes to the production environment without online action by a second user.

Finally, organizations must be particularly careful to disable access by former system administrators and privileged users. Thoroughly-documented procedures for disabling access can help ensure that stray access points are not overlooked. In addition, the two-person rule should be considered for the critical functions performed by these users to reduce the risk of extortion after they leave the organization.

Case Study

A system administrator at an international financial organization heard rumors that the annual bonuses were going to be lower than expected. He constructed a logic bomb at home and used authorized remote access to move the logic bomb to the company's servers as part of the typical server upgrade procedure. The upgrade process occurred over a period of two and a half months.

When he was informed by his supervisor that his bonus would be significantly lower than he had expected, he terminated his employment immediately. Less than two weeks later, the logic bomb went off at 9:30 a.m., deleting 10 billion files on approximately 1,000 servers throughout the United States.

The organization estimated that it would cost more than \$3 million to repair its network, and the loss affected 1.24 billion shares of its stock.

Case Study

One insider was promoted from one position to another within the same organization. Both positions utilized the same application for entering, approving, and authorizing payments for medical and disability claims. The application used Role Based Access to enforce separation of duties for each system function. However, when this particular insider was promoted, she was authorized for her new access level, but administrators neglected to rescind her prior access level (separation of duties was inadequately enforced). As a result, she ended up having full access to the application, with no one else required to authorize transactions (payments) from the system.

She entered and approved claims and authorized monthly payments for her fiancé, resulting in payments of over \$615,000 over almost two years.

Actively Defend Against Malicious Code

While insiders frequently use simple user commands to do their damage, logic bombs and other malicious code are used frequently enough to be of concern.

Many organizations defend against malicious code using antivirus software and host or network firewalls. While these defenses are useful against external infections, their value is limited in preventing attacks by malicious insiders in two important respects: They do not work against new or novel malicious software (including destructive software logic bombs planted by insiders); and they are concerned primarily with material spread through networking interfaces, rather than material installed directly on a machine. To deal with these limitations, a more systematic and active approach is needed.

First, organizations should identify baseline software and hardware configurations. A given organization may have several baseline configurations, given the different computing and information needs of different users (accountant, manager, programmer, receptionist). But as configurations are identified, the organization should characterize the hardware and software that makes up those configurations.

The characterization can be simply a catalog of information, such as versions of installed software, hardware devices, and disk utilization. However, very basic characterizations are often simple to defeat, so more comprehensive characterizations are often required.

These characterizations include:

- Cryptographic checksums (using [SHA1](#) or [MD5](#), for example).
- Interface characterization (such as memory mappings, device options, and serial numbers).
- Recorded configuration files.

Once this information is captured, computers implementing each configuration can be validated by recollecting the information and comparing it against the baseline copy. Any discrepancies can then be investigated to determine whether they are benign or malicious. Using these techniques, changes to system files or the addition of malicious code will be flagged for investigation.

[Tools](#) called file [integrity checkers](#) partially automate this process and provide for scheduled sweeps through computer systems.

Computer configurations do not remain fixed and unchanged for very long. Therefore, characterization and validation should be part of an organization's configuration management process.

For protection against malicious insiders, part of the configuration management process should be separation of duties. For example, validation of a configuration should be done by a person other than the one who made changes so that there is some opportunity to detect and correct malicious changes (planting logic bombs).

Case Study

A system administrator at a manufacturing firm began his employment as a machinist. Because of his technical ability he also, over a ten-year period, created the company's network from scratch and had sole authority for system administration. The company eventually expanded and began to open additional offices and plants, both nationally and internationally.

The insider:

- Began to feel disgruntled at his diminishing importance to the company.
- Launched verbal and physical assaults on coworkers.
- Sabotaged projects for which he was not in charge.
- Loaded faulty programs to make coworkers look bad.

He received a verbal warning, two written reprimands, was demoted, and was finally fired as a result of his actions. A few weeks later a logic bomb was released on the company's network that deleted one thousand critical manufacturing programs from the company's servers.

The company estimated the cost of damage in excess of \$10 million, which led to the layoff of approximately 80 employees. The investigation revealed that the insider had actually run a test version of the logic bomb three times on the company's network prior to his termination.

Practices for detection of malicious code would have detected that a new program had been released to the network with timed release. Configuration control procedures could have enforced a two-person rule for release of system-level programs, and configuration characterization and monitoring could have permitted detecting the release of a new system file that was not part of the original system baseline.

Case Study

An organization had automated logging and monitoring built into its custom-developed software that sent automatic notification to the security officer any time a highly-restricted function was used to modify information stored in the database. Role based access control restricted access to this function to only a few very high level users, and the automated notification provided a second layer of defense against illegal modification of data using that function.

However, one of the developers of the application, who also happened to have access to that function, modified the code so that the automated notification was no longer sent. He then proceeded to use the function to steal a large sum of money from his employer.

Interestingly, the organization also had a comprehensive logging system in place for software changes. Any time a program was compiled, a report was produced listing which files were compiled, by which computer account, and when. It also listed which modules were added, modified, or deleted.

Unfortunately, this report was not monitored, and therefore the changes made to the application were not detected during the year and a half over which the fraud was committed. Had it been monitored, or had a configuration control system been in place to enforce the two-person rule for releasing new versions of software, the removal of the security notification would have been detected and the insider could not have committed the fraud.

Use Layered Defense Against Remote Attacks

Remote access provides a tempting opportunity for insiders to attack with less risk.

Insiders often attack organizations remotely using access provided by the organization, or following termination. While remote access can greatly enhance employee productivity, caution is advised when remote access is provided to critical data, processes, or information systems.

Insiders have admitted that it is easier to conduct malicious activities from home because it eliminates the concern that someone could be physically observing the malicious acts.

The vulnerabilities inherent in allowing remote access suggest that multiple layers of defense should be built against remote attack. Organizations may provide remote access to email and noncritical data but should strongly consider limiting remote access to the most critical data and functions.

Access to any data or functions that could inflict major damage to the company should be limited to employees physically located inside the workplace. This should be the rule rather than the exception. Remote system administrator access should be limited to the smallest group practicable, if not prohibited altogether.

When remote access to critical data, processes, and information systems is deemed necessary, the organization should offset the added risk with closer logging and frequent auditing of remote transactions. Information such as login account, date/time connected and disconnected, and IP address should be logged for all remote logins. It also is useful to monitor failed remote logins, including the reason the login failed. If authorization for remote access to critical data is kept to a minimum, monitoring can become more manageable and effective.

Disabling remote access is an often overlooked but critical part of the employee termination process. It is critical that employee termination procedures include:

- Disabling remote access accounts (such as VPN and dial-in accounts).
- Disabling firewall access.
- Changing the passwords of all group accounts (including system administrator, database administrator (DBA), and other privileged group accounts).
- Closing all open connections.

A combination of remote access logs, source IP addresses, and phone records usually helps to identify insiders who launch remote attacks. Identification can be straightforward because the user name of the intruder points directly to the insider.

Of course, corroboration of this information is required, because the intruders might have been trying to frame other users, cast attention away from their own misdeeds by using other users' accounts, or otherwise manipulate the monitoring process.

Case Study

For a period of five years, a foreign currency trader with an investment bank "fixed" the bank's records to make his trading losses look like major gains for the bank. His actions made it appear that he was one of the bank's star producers, resulting in lucrative bonuses for his perceived high performance.

In actuality, the bank lost hundreds of millions of dollars and drew a large amount of negative media attention as a result of his actions. While initially most of the insider's fraud occurred at work, he increasingly found it easier to conduct his illicit activities from home in the middle of the night because he did not have to worry about anyone in the office or at home looking over his shoulder.

Therefore, the risk that other traders would find out about his fraudulent activities was reduced significantly.

In an interview for the Insider Threat Study, the insider said that group trading (trading by a team of traders), rather than individual trading, can help mitigate an organization's risks, because it is easier to detect illegal or suspicious trading practices when there [are multiple team members trading from the same account.](#)

In this case isolated trading, along with the anonymous nature of remote access, emboldened the insider to continue a fraud in which he otherwise might not have engaged.

Case Study

A government organization notified one of its contract programmers that his access to a system under development was being eliminated and that his further responsibilities would be limited to testing activities. After his protests were denied, the programmer quit the organization. Then, three times over a two-week period, the insider used a backdoor into the system with administrator privilege (which he presumably installed before leaving) to download source code and password files from the developmental system.

The unusually large size of the remote downloads raised red flags in the organization, which resulted in an investigation that traced the downloads to the insider's residence and led to his arrest, prosecution, and imprisonment. This case demonstrates the value of vigilant monitoring of remote logs and action on suspicious behavior to limit damage to the organization's interests.

Monitor and Respond to Suspicious or Disruptive Behavior

One method of reducing the threat of malicious insiders is to proactively deal with destructive employee behaviors.

An organization's methods of dealing with these behaviors originates in the hiring process.

Consistent background checks and evaluation of the results can reduce insider threats. The background checks should investigate previous criminal convictions and verify credentials and past employment. The background check should include discussion with prior employers regarding the individual's competence and approach to dealing with issues in the workplace. While this information may not be the dominant component in the hiring process (and, arguing fairness, should not be), the information gathered may help in dealing proactively with the individual. Research has revealed a surprisingly [high number of malicious insiders who had prior criminal convictions when hired](#).

Proactive management should not be punitive in nature; rather, the individual should be cultivated into the organizational climate with appropriate care and thoroughness.

After employment, if an employee's behavior becomes suspicious, the organization must act with due care. Policies and procedures must exist for employees to report their concerns or to report disruptive behavior by others to a single contact point enterprise-wide, and reports should always be investigated. (Some checks and balances must exist to limit frivolous reporting.) Disruptive employees should not be allowed to migrate from one position to another within the enterprise in order to evade documentation of disruptive activity.

Threats, malicious boasting ("You wouldn't believe how easily I could trash this net!") and other negative sentiments should also be treated as disruptive or potentially destructive behavior.

All employees have concerns and/or grievances, and a formal and accountable process for addressing those concerns and grievances may act to satisfy those who might otherwise resort to malicious activity.

Once a disruptive/destructive behavior is identified, several steps can aid the organization in managing malicious activity risk. First, the employee's access to critical information assets should be evaluated. His or her level of network access should also be considered.

While this is done, the organization must provide options to the individual for coping with the behavior, including access to a confidential employee assistance program.

Case Study

A system administrator was hired to run the engineering department for an organization and three months later, named as the lead for a major new project. He then began to act in a bullying manner to his co-workers, and was taken off the project a month after it started. Less than two months after that, he was terminated for poor performance and conduct.

Customers had complained that he was rude, and co-workers said that he thought he was better than everyone else. His superiors realized that he was not as good technically as they had originally believed and suspected that he was attempting to hide that fact by criticizing others. The company did provide counseling, but he resented it.

Almost two months after his termination, the insider obtained a system administrator account password from a female employee who was still with the company, with whom he'd had a relationship. Using this password, the insider was able to hide the project folder on the server that was needed the next day for an important customer demonstration.

Although the company did employ standard recommendations in handling this insider, he still managed to sabotage the company's system. This case highlights the fact that companies should consider social relationships that terminated insiders have with employees still working for the company.

Case Study

One insider was a vice president for engineering and responsible for oversight of all software development in the company. He was engaged in a long-running dispute with higher management.

This dispute was characterized by verbal attacks by the insider and statements to colleagues about the degree of upset he had caused to management. The insider engaged in personal attacks once or twice a week and on one occasion in a restaurant screamed personal attacks at the company CEO. A final explosive disagreement led the insider to quit.

When no severance package was offered, he copied a portion of a product under development to removable media, deleted it from the company's server, and removed the recent backup tapes. He then offered to restore the software in exchange for \$50,000. He was charged and convicted of extortion, misappropriation of trade secrets, and grand theft.

However, the most recent version of the software was never recovered. If the organization had paid attention to earlier disruptive behavior and acted to secure assets against his access, substantial losses could have been avoided.

Deactivate Computer Access Following Termination

While employed, insiders have legitimate, authorized access to the organization's network, system, applications, and data. Once employment is terminated (whether under favorable or unfavorable circumstances), the organization must execute rigorous termination procedures that disable all open access points.

Otherwise, the organization's network is vulnerable to access by a now-illegitimate, unauthorized user.

If formal termination policies and procedures are not in place, the termination process tends to be ad hoc, posing significant risk that one or more points of access will be overlooked.

Research in the [Insider Threat Study](#) shows that insiders can be quite resourceful in exploiting obscure access mechanisms that were neglected in the termination process. Once a formal process is established, it must be strictly followed for all terminations.

It is also critical that organizations remain alert to new insider threat research and periodically review and update these processes.

Some aspects of the termination process are quite obvious, such as disabling the terminated employee's computer account. However, organizations that have been victims of insider attacks were often vulnerable because of poor, nonexistent, or non-comprehensive account management procedures. Many employees have access to multiple accounts; all account creations should be tracked and periodically reviewed for accuracy to ensure that all access can be quickly eliminated when an employee is terminated.

Accounts that are sometimes overlooked in the termination process are **group** accounts. Group accounts are typically shared among multiple users to implement a two-person rule.

Examples of such accounts are System Administrator accounts and DBA accounts. In addition, some applications require administrative accounts that are frequently shared among multiple users. It is important that the organization meticulously maintain a record of every shared account and every user who knows the password to each.

Remote access is another frequently-exploited access point. Remote access or Virtual Private Network (VPN) accounts must be disabled, as well as firewall access, in order to prevent future remote access by the terminated employee. In addition, any remote connections already open by that employee must be closed immediately.

In summary, a layered defensive model that accounts for all access methods should be implemented. Remote access should be disabled, but if an obscure remote access method is overlooked, the next layer of defense is accounts. All accounts should be disabled, so that even if remote access is established, the insider is prevented from proceeding further.

Intranet accounts, application specific accounts, and all other accounts for which the user was authorized must be disabled. Also, keep in mind that if the terminated insider was responsible for establishing accounts for others, such as employees, customers, or external website users, then those accounts could also be accessible to the terminated insider.

Finally, termination procedures must include steps to prevent physical access. Some insiders have been known to exploit physical access as a means of gaining access to their former employer's computer system.

Case Study

The system administrator at a credit union was terminated suddenly, with no previous notice that his employer was dissatisfied with his work. That night he suspected that his replacement, who he felt was technically inferior, had not disabled his access. He attempted to access the system from his home and found that his replacement had failed to disable his access through the company firewall.

Although his replacement had disabled his user account, she had failed to change the password of the system administrator account. The insider used that account to shut down the organization's primary server, one that had been having problems and had in fact crashed the previous weekend (which had taken him an entire weekend to bring up again). It took the credit union three days to bring the server back into service; during that time none of its customers were able to access the money in any of their accounts in any way.

This case illustrates the necessity of thoroughly disabling access, as well as the consequences when an organization has no competent backup for a single system administrator.

Case Study

A system administrator logged in one morning and was notified by her custom-written login software that she had last logged in one hour before.

This set off immediate alarms, as she had in fact not logged in for several days. She had previously taken steps to discretely redirect logging of actions by her account to a unique file rather than the standard shell history file. Therefore, she was able to trace the intruder's steps and saw that the intruder had read another employee's email using her account and then deleted the standard history file for her account so that there would be no log of his actions.

The login was then traced to a specific computer that happened to be located physically at a subsidiary of the company. Further investigation showed that the same computer had logged into the company's system periodically for the past month.

Active monitoring by both the victim company and the subsidiary then showed that a former employee of the victim organization had accessed up to sixteen computer systems belonging to his former employer. This access occurred on a daily basis during working hours.

The insider did the following:

- Gained access to at least 24 user accounts.
- Read electronic mail.

- Reviewed source code for his previous project.
- Deleted two software modification notices for the project.

The former employee had been terminated for nonperformance and then went to work for the subsidiary. This case illustrates the importance of terminating access completely for former employees, careful monitoring for post-termination access, and paying particular attention to terminated technical employees.

Collect and Save Data for Use in Investigations

Collecting and saving usable evidence preserves response options, including legal options.

The first questions that often follow any computer incident, whether malicious or not, are "what happened?" and "who is responsible?" In the cases where malicious insiders are suspected, these questions are particularly urgent. Answering these questions in an actionable manner requires a detailed record of system and network actions.

However, malicious insiders may act to corrupt, falsify, or delete such a record, impacting options for corrective and responsive actions.

To best protect critical information and equipment, multiple sources of information should be maintained, particularly sources that may support one another. This includes logging the following information:

- Data access (reading, modifying, or deleting data).
- Application usage (when applications were started and exited and by which user).
- System commands and file change logs.
- Method of connection (console, local-area networked, dial-in, Internet).
- The source and destination of connections.

Phone system and physical access records should also be maintained. As this information is collected, it should also be placed on backup media for archival storage.

As difficult as collecting all this information is, analysis is often harder. The signs of malicious insider activity can be subtle, such as an abnormal pattern or rate of data modification, or an off-hours download of information the insider is authorized to read. Log files need to be monitored periodically to try to identify such situations. Unfortunately, many of the publicly-available log file analysis tools are not designed for this type of analysis.

Organizations may need to involve a forensics specialist, both to design a routine analysis procedure for identifying malicious insiders, and for more specialized analysis once the insider is identified. Insider threat cases have occurred in which inappropriate handling of system logs has rendered them unacceptable for prosecution. In the event of a suspected security incident, involve an expert in the investigation of electronic crimes.

Case Study

An employee of a subcontractor for a government agency was nearing completion of his contract. Ordinarily, under these circumstances, the government agency would offer the employee a permanent position if his or her performance had been satisfactory working for the subcontractor.

The insider initiated this hiring process and was required to take a drug test. The drug test results came back positive for cocaine, so his employment possibilities for the agency were forfeited. He remained employed with his current employer for a few days until that organization was notified of his drug test results and terminated his employment immediately.

His physical access cards were confiscated, he was escorted from the building, his personal computer account was disabled, and the password was changed on the system administrator account to which he had access.

The following Monday morning, the subcontractor's system was down. The logs showed that the system had been shut down via commands from a bogus account that was not associated with any legitimate user. Remote access logs showed that attempts to log in began Friday evening and continued through early Saturday before being successful.

Once authenticated, the user had deleted a number of printer drivers in the system, altered and changed certain user passwords, and finally entered the command to shut down the system. The logs on the remote access server stored the phone number of the incoming connections, and it was traced to the home address of the terminated insider. These logs were key in successfully prosecuting the insider.

Case Study

In contrast to the above case, where logs were stored appropriately and used to identify the user for prosecution, the following case illustrates the opposite case:

A contractor for a large company was responsible for handling customer service calls. A fraud scheme conducted by four employees over a period of almost three years resulted in losses for the company of \$500,000.

However, once the fraud was suspected by the company's fraud investigator, it was discovered that, since the company "recycled" its computer logs, they only provided specific activity by login name and computer terminal as far back as one month. Fortunately, one of the employees involved testified as to the history and duration of the fraud.

This case illustrates the importance of securely backing up system logs for long time periods in case they are needed for investigations or prosecution.

Implement Secure Backup and Recovery Processes

Despite all precautions implemented by an organization, it is still possible that an insider will attack. Therefore, it is important that organizations prepare for that possibility by implementing secure backup and recovery processes that are tested periodically.

Prevention of insider attacks is the first line of defense. However, experience has taught that attacks can be prevented only up to a point. Unfortunately, there will always be avenues for an insider to successfully compromise a system. Effective backup and recovery processes need to be in place and operational so that if compromises do occur business operations can be sustained with minimal interruption.

Research has shown that effective backup and recovery mechanisms can make the difference between several hours of downtime to restore systems from backups and weeks of manual data entry when backups are not available.

When possible, multiple copies of backups should exist, with redundant copies stored off-site in a secure facility.

Different people should be responsible for the safekeeping of each copy so that it would require the cooperation of multiple individuals to compromise the means to recovery.

System administrators should ensure that the physical media on which backups are stored are also protected from insider corruption or destruction. Insider cases in our research have involved attackers who did the following:

- Deleted backups.
- Stole backup media.
- Performed actions that could not be undone due to faulty backup systems.

Some system administrators neglected to perform backups in the first place, while others sabotaged established backup mechanisms. Such actions can amplify the negative impact of an attack on an organization by eliminating the only means of recovery.

To guard against insider attack, organizations must ensure that:

- Backups are performed and periodically tested.
- Media and content are protected from modification, theft, or destruction.
- Separation of duties and configuration management procedures are applied to backup systems just as they are to other system modifications.

Unfortunately, attacks against networks may interfere with common methods of communication, thereby increasing uncertainty and disruption in organizational activities, including recovery from the attack. This is especially true of insider attacks, since insiders are quite familiar with organizational communication methods and, during attack, may interfere with communications essential to the organization's data backup process.

Organizations can mitigate this effect by multi-homing, an approach that maintains trusted communication paths outside of the network with sufficient capacity to ensure critical operations in the event of a network outage. This protection provides two benefits: the cost of strikes against the network would be mitigated, and insiders would be less likely to strike against connectivity because of the reduced impact.

Case Study

Centralization of critical assets and sabotage of backups has enabled some insiders to amplify the impact of their attacks by eliminating redundant copies and avenues for recovery. One insider, the sole system administrator, centralized the only copy of all of the company's critical production programs on a single server and instituted policies mandating this practice.

That server was later the target of a logic bomb written by the same insider. No other current copy of the software was available to recover from the attack, since he had also requested and received, through intimidation, the only backup tape, violating company policy.

The logic bomb, which deleted all of the company's programs, cost the company millions of dollars and caused company-wide layoffs. While centralization can contribute to the efficiency of an organization, care must be taken that backups are performed regularly and are protected to ensure business continuity in the event of damage to or loss of centralized data.

Case Study

This case illustrates the delay that can be caused in recovery following an insider attack if backups are not tested periodically.

An insider was terminated because of his employer's reorganization. The company followed proper procedure by escorting the insider to his office to collect his belongings and then out of the building. The IT staff also followed the company's security policy by disabling the insider's remote access and changing passwords.

However, they overlooked one password that was known to three people in the organization; the terminated insider used that account to gain access to the system that night and to delete the programs that he had created while working there. Some of these programs supported the company's critical applications.

Restoration of the deleted files from backup failed. While the insider had been responsible for backups, company personnel believe that the backups were not maliciously corrupted. The backups had simply not been tested to ensure that they were properly recording the critical data. As a result, the organization's operations in North and South America were shut down for two days, causing more than \$80,000 in losses.

Clearly Document Insider Threat Controls

To ensure consistent handling and to protect against accusations of discrimination, procedures for dealing with malicious insiders must be clearly documented.

Cases involving malicious insiders are difficult to handle. Relationships between management and employees may be strained, with individuals taking sides with the organization or with the employee. A clearly-written set of policies and procedures, developed with protection of the rights of everyone involved in mind, may help to defuse this situation.

All of the organization's efforts to control damage by malicious insiders should be identified, together with circumstances under which these efforts are appropriate. As individuals join the organization, they should receive a copy of this description that clearly lays out what is expected of them, together with the consequences of violations. Evidence that each individual has read and agreed to the organization's policies, such as the individual's signature, should be maintained.

This description should also form the basis of ongoing training as described in the first practice. If the organization experiences damage due to a malicious insider or if other risks evolve, such as new forms of internal or external attack, the description and training should be updated.

The training must be delivered periodically to all employees, to help individuals act properly.

Case Study

An insider accepted a promotion, leaving a system administrator position in one department and taking a position as a systems analyst in another department of the same organization.

In his new position, he was responsible for information sharing and collaboration between his old organization and the new one. The following events ensued:

- The original department terminated his system administrator account and issued him an ordinary user account to support the access required in his new position.
- Shortly thereafter, the system security manager at the original department noticed that the former employee's new account had been granted unauthorized administrative rights.
- The security manager reset the account back to ordinary access rights, but a day later found that administrative rights had been granted to it once again.
- The security manager closed the account, but over the next few weeks other accounts exhibited unauthorized access and usage patterns.

An investigation of these events led to charges brought against the analyst for misuse of computing systems. These charges were eventually unsuccessful, in part because there was no clear policy regarding account sharing or exploitation of vulnerabilities to elevate account privileges.

This case illustrates the importance of clearly established policies that are consistent across departments, groups, and subsidiaries of the organization.

C H A P T E R 3

Developing the ICS Security Program

Critical operational differences have been identified between ICS and IT systems that influence how specific security measures should be applied to the ICS.

Accordingly, organizations should develop and deploy an ICS security business case that describes program elements, costs, and expected results.

ICS security plans and programs should leverage existing IT security experience, programs, and practices. The ICS plans and programs should be tailored to the specific requirements and characteristics of ICS technologies and environments. Organizations should review and update their ICS security plans and programs regularly to incorporate changes in technologies, operations, standards, and regulations, as well as the security needs of specific facilities.

Developing the ICS Security Program includes creating a business case that articulates the specific security needs and cost benefits of the Program. This chapter provides an overview of the development and distribution of a detailed ICS security business case, and considerations of identifying the Security Program best suited to your environment.

Contents

- Developing the ICS Security Business Case
- Developing a Comprehensive Security Program
- Managing Risk
- Creating ICS Security Controls

Developing the ICS Security Business Case

The first step to implementing a cyber security program for ICS is to develop a compelling business case for the unique needs of the organization.

The business case should capture the business concerns of senior management while being founded in the experience of those who are already dealing with many of the same risks. The business case provides the business impact and financial justification for creating an integrated cyber security program. It should include detailed information about the following:

- Benefits of creating an integrated security program.
- Prioritized potential costs and damage scenarios if a system is not put into place.
- Costs and resources required to develop and implement the security program.
- High-level overview of the process required to implement, operate, monitor, review, maintain, and improve the cyber security program.

Before presenting the business case to management, develop a well-thought-out and detailed security implementation plan. Simply requesting a firewall is generally insufficient.

Defining ICS Security Benefits

Responsible risk management mandates that threats to the ICS should be measured and monitored to protect the interests of employees, the public, shareholders, customers, vendors, and the larger society. Risk analysis enables costs and benefits to be weighed so that informed decisions can be made on protective actions. In addition to reducing risks, displaying responsibility also helps companies by:

- Improving employee morale, loyalty and retention.
- Addressing community concerns.
- Increasing investor confidence.
- Reducing legal liabilities.
- Enhancing the corporate image and reputation.
- Helping with insurance coverage.
- Improving investor and banking relations.

Proactive measures by companies can also help forestall new and more prescriptive regulations that increase costs and impede business flexibility. A strong safety and security management system is fundamental to a sustainable business model.

Defining Potential Impacts and Consequences

The importance of secure systems cannot be over-emphasized as business reliance on inter connectivity increases. Denial of service attacks, worms, and viruses have become all too common and have already impacted the sector. In addition, a cyber breach in some sectors can have significant physical impacts, such as the following.

- **Physical Impacts:** Physical impacts encompass the set of direct consequences of ICS mis-operation. The potential effects of paramount importance include personal injury and loss of life. Other effects include the loss of property (including data) and damage to the environment.
- **Economic Impacts:** Economic impacts are a second-order effect from physical impacts ensuing from cyber intrusion. Physical impacts could result in repercussions to system operations, which in turn inflict a greater economic loss on the facility or company. On a larger scale, these effects could negatively impact the local, regional, national, or possibly global economy.
- **Social Impacts:** Another second-order effect, the loss of national or public confidence in an organization is often overlooked. It is a very real target and one that can be accomplished through cyber attack. Social impacts may possibly lead to heavily depressed public confidence or the rise of popular extremism.

A list of potential consequences of cyber attacks against an ICS is as follows:

- Impact on national security - facilitate an act of terrorism.
- Reduction or loss of production at one site or multiple sites simultaneously.
- Injury or death of employees.
- Injury or death of persons in the community.
- Damage to equipment.
- Release, diversion, or theft of hazardous materials.
- Environmental damage.
- Violation of regulatory requirements.
- Product contamination.
- Criminal or civil legal liabilities.
- Loss of proprietary or confidential information.
- Loss of brand image or customer confidence.

Undesirable incidents of any sort detract from the value of a business, but safety and security incidents can have longer-term negative impacts than other types of incidents on *all* stakeholders-employees, shareholders, customers, and communities in which a company operates.

Safety and security are simply good business.

Key Business Case Components

Include the following key business case components: prioritized threats, prioritized business consequences, and estimated annual business impact.

Prioritized Threats

The list of potential threats provided in a previous section must be refined, if possible, to include only those threats that are deemed credible to the company. For example, a food and beverage company might not find terrorism a credible threat but might be more concerned with viruses, worms, and disgruntled employees.

Prioritized Business Consequences

The list of potential business consequences provided in a previous section must be distilled to include only the particular business consequences that senior management find the most compelling. For example, a food and beverage company that handles no toxic or flammable materials and typically processes its product at relatively low temperatures and pressures might not be concerned about equipment damage or environmental impact, but might be more concerned about loss of production availability and degradation of product quality.

Regulatory compliance might also be a concern. The [Sarbanes Oxley Act](#) requires corporate leaders to sign off on compliance with information accuracy and protection of corporate information. The demonstration of due diligence is required by most all internal and external audit firms to satisfy shareholders and other company stakeholders.

Estimated Annual Business Financial Impact

The highest-priority items shown in the list of prioritized business consequences should be evaluated to obtain an estimate of the annual business impact preferably, but not necessarily, in financial terms.

For the food and beverage company example, it may have experienced a virus incident within its internal network that the information security organization estimated as resulting in a specific financial cost. Since the internal network and the control network are interconnected, it is conceivable that a virus originating from the control network could cause the same amount of business impact.

Building the Business Case

The two main resources for information to help form a business case are external resources in trade organizations, and internal resources in related risk management programs or engineering and operations.

External resources in trade organizations can often provide useful tips as to what factors most strongly influenced their management to support their efforts, and what resources within their organizations proved most helpful.

These factors may be different between industries, but there may be similarities in the roles that other risk management specialists can leverage.

Internal resources in related risk management efforts (information security, health, safety and environmental risk, physical security, business continuity, etc.) can provide tremendous assistance based on their experience with related incidents in the organization. This information is helpful from the standpoint of prioritizing threats and estimating business impact.

Internal resources can also provide insight into which managers are focused on dealing with which risks and, thus, which managers might prove the most appropriate or receptive to serving as a champion.

Internal resources in control systems engineering and operations can provide insight into the details of how control systems are deployed within the organization, including the following details:

- How networks are typically segregated.
- How high-risk combustion systems or safety instrumented systems are typically designed.
- What security countermeasures are commonly used

Presenting the Business Case to Leadership

Present the business case to leadership for IT, industrial control systems, value chains, and third party stakeholders. Obtain buy-in and support from all involved parties, and determine how funding requirements will be divided. The business leadership will be responsible for approving and driving cyber-security policies, assigning security roles, and implementing the cyber-security program across the company.

Funding Considerations

Funding for the entire program can usually be done in phases. While some funding may be required to start the cyber-security activity, additional funding can be obtained later as the security vulnerabilities and needs of the program are better understood, and as additional strategies are developed.

Leveraging Case Studies

A good approach to obtain management buy-in is to ground the business case in a successful actual third party example. The business case should present that the other organization had the same problem and then present that they found a solution and how they solved it. This will often prompt management to ask what the solution is and is it applicable to their organization.

Developing a Comprehensive Security Program

Effectively integrating security into an ICS requires defining and executing a comprehensive program that addresses all security aspects, ranging from identifying long-term objectives, to day-to-day operation and ongoing auditing for compliance and improvement.

This section describes the basic process for developing a security program, including the following tasks:

- Building a Cross-Functional Team
- Defining Charter and Scope
- Defining Policies and Procedures
- Defining ICS Assets
- Performing the Vulnerability Assessment
- Defining the Mitigation Controls
- Providing Training and Security Awareness

Note More detailed information on the various steps is provided in Part 2 of the ISA SP99 Standard and ISA TR99.00.02: Integrating Electronic Security into the Manufacturing and Control Systems Environment.

The commitment to a security program begins at the top. Senior management must demonstrate a clear commitment to cyber security. Cyber-security is a business responsibility shared by all members of the enterprise and especially by leading members of the business, process, and manufacturing management teams. Cyber-security programs with visible, top-level support from organization leaders are more likely to gain compliance, function more smoothly, and have earlier success.

Whenever a new system is being installed, it is imperative to take the time to address security from the very beginning and address it throughout the life cycle from architecture to procurement to installation to maintenance to decommissioning.

There are serious risks in deploying systems to production based on the assumption that they will be secured later: If there are insufficient time and resources to secure the system properly before deployment, it is unlikely that there will be sufficient time and resources later.

Building a Cross-Functional Team

It is essential for a cross-functional Cyber-Security team to share their varied domain knowledge and experience to evaluate and mitigate risk in the ICS. The cyber-security team should consist of a member of the organization's IT staff, a process engineer, and a member of the management staff at a minimum. For continuity and completeness, the cyber security team should include the process control system vendor.

The cyber security team should report directly to site management and determine accountability. Management level accountability will help ensure an ongoing commitment to cyber-security efforts.

While the process engineers will play a large role in securing the ICS, they will not be able to do so without collaboration and support from both the IT department and management. A good team-building exercise would be to invite IT and management down to the operations floor for coffee and donuts and to share their varied domain knowledge and experience to develop the ICS security program.

Defining Charter and Scope

The Cyber-Security team should establish the corporate policy that defines the guiding charter of the security organization and the roles, responsibilities, and accountabilities of system owners and users.

The team should decide upon and document the objective of the security program, the business organizations affected, all the computer systems and networks involved, the budget and resources required, and the division of responsibilities. The scope can also address business, training, audit, legal, and regulatory requirements, as well as timetables and responsibilities.

There may already be a program in place or being developed on the IT side of the company. The team should identify which existing practices to leverage and which practices are specific to the control system. In the long run, it will be easier to get positive results if the team can share resources with others in the company who have similar objectives.

Defining Policies and Procedures

Policies and procedures are at the root of every successful security program. Policies and procedures help to ensure that security protection is both consistent and current, to protect against evolving threats, and to educate. After the risks for the various systems are clearly understood, the cyber security team should examine existing security policies to see if they adequately address the risks.

Existing policies should be revised or new policies created to address desktop and business systems, industrial control systems, and value-chain systems. Few companies have the resources to harden the ICS against all possible threats; management must guide the development of the security policies that will set the security priorities and goals for the organization so that the risks posed by the threats are mitigated sufficiently.

Procedures that support the policies must be developed so that the policies are implemented fully and properly for the ICS. Security procedures should be well-documented and tested, and they should be updated periodically, and as needed in response to policy and technology changes.

Defining ICS Assets

The Cyber-Security team should identify the applications and computer systems within the ICS, as well as the networks within and interfacing to the ICS.

The focus should be on systems rather than just devices, and should include PLC, DCS, and instrument-based systems that use a monitoring device such as an HMI. Assets that use a routable protocol or are dial-up accessible must be documented. As the team identifies the process control systems, the information should be recorded in a standardized format. The team should review and update the ICS asset list annually.

Several commercial enterprise-inventory tools are available to identify and document all hardware, systems, and software resident on a network. Care must be taken before using these tools to identify ICS assets: Teams should conduct an assessment of how these tools work and what impact they might have on the connected control equipment before using any of them.

Tool evaluation may include testing in similar, non-production control system environments to ensure that the tools do not adversely impact the production systems. Impact could be due to the nature of the information or the volume of network traffic. While this impact may be acceptable in IT systems, it is not acceptable in an ICS.

Performing the Vulnerability Assessment

Because every company has a limited set of resources, organizations should perform a risk assessment for the ICS systems and use its results to prioritize the ICS systems. The organization should then perform a detailed vulnerability assessment for the highest-priority systems.

The vulnerability assessment will help identify any weaknesses that may be present in the systems that could allow inappropriate access to systems and data, along with the related cyber security risks and mitigation approaches to reduce the risks.

Because of the potential for disruption to the devices, [vulnerability scanners should be used with caution on production ICS networks](#). Accidental denial of service to devices and networks is major concern in this context: Vulnerability scanners often attempt to verify vulnerabilities by extensively probing and conducting a representative set of attacks against devices and networks. These systems were designed and built to control and automate real world processes or equipment.

Given the wrong instructions, they could perform an incorrect action, causing waste, equipment damage, injury, or even deaths.

The following examples demonstrate this danger:

- While a ping sweep was being performed on an active SCADA network that controlled 9-foot robotic arms, it was noticed that one arm became active and swung around 180 degrees. The controller for the arm was in standby mode before the ping sweep was initiated. Luckily, the person in the room was outside the reach of the arm.
- A ping sweep was performed in an ICS network to identify all hosts that were attached to the network (for inventory purposes), and it caused a system controlling the creation of integrated circuits in the fabrication plant to hang. The outcome was the destruction of \$50K worth of wafers.
- A gas utility hired an IT security consulting company to conduct penetration testing on their corporate IT network and carelessly ventured into a part of the network that was directly connected to the SCADA system. The penetration test locked up the SCADA system and the utility was not able to send gas through its pipelines for four hours. The outcome was the loss of service to its customer base for those four hours.

ICS Vulnerability Assessment Summary

Identifying the vulnerabilities within an ICS requires a different approach than in a typical IT system. In most cases, devices on an IT system can be rebooted, restored, or replaced with little interruption of service to their customers. An ICS controls a physical process and therefore has real world consequences associated with its actions. Some actions are time-critical, while others have a more relaxed time frame.

When performing an inventory or vulnerability scan on an IT system, several steps are generally performed. Each step is listed in the following table, along with the usual IT action and alternate/suggested actions that should be taken for an ICS, making the outcomes of any testing predictable and safe. These techniques may make the work somewhat more difficult, but should help to mitigate problems associated with active scanning:

To Be Identified	IT Action	Suggested ICS Action
Hosts, nodes, and networks.	Ping sweep (e.g., nmap)	<ul style="list-style-type: none"> • Examine router configuration files or route tables. • Perform physical verification (chasing wires). • Conduct passive network listening or use intrusion detection (e.g., snort) on network.
Services	Port scan (e.g., nmap)	<ul style="list-style-type: none"> • Do local port verification (e.g., netstat). • Scan a duplicate, development, or test system on a non-production network.
Vulnerabilities within a service.	Vulnerability scan (e.g., nessus)	<ul style="list-style-type: none"> • Perform local banner grabbing with version lookup in Common Vulnerabilities and Exposures (CVE) • Scan a duplicate, development, or test system on a non-production network.

The commonality among the suggested ICS actions is that they do not generate traffic on production operational networks or against production systems. These less intrusive methods can gather most, if not all, of the same information as more active methods, without the risk of causing a failure by testing.

Another factor to consider when choosing ICS testing methods is that these systems have very limited resources as compared to normal IT systems. ICS systems have much greater longevity than their IT counterparts, so their hardware is often well behind the state-of-the-art and can be easily overtaxed. Also, ICS systems usually run at slow speeds on legacy networks that can be overwhelmed by the volume of traffic generated during active testing.

When any assessment of the ICS is being performed, ICS personnel must be aware that testing is occurring, and be prepared to immediately address any problems that arise:

- If manual control of the system is possible, personnel capable of performing manual control must be present during the security testing.
- Security auditors need to understand the ICS under test, the risk involved with the test, and the consequences associated with unintentional stimulus or denial of service to the ICS.

Defining the Mitigation Controls

Organizations should analyze the detailed risk assessment, identify the cost of mitigation for each risk, compare the cost with the risk of occurrence, and select those mitigation controls where cost is less than the potential risk. Because it may be impractical or impossible to eliminate all risks, organizations should focus on mitigating the risk for the most critical applications and infrastructures.

The controls to mitigate a specific risk may vary among types of systems. For example, user authentication controls might be different for ICSs than for corporate payroll systems and e-commerce systems.

Organizations should document and communicate the selected controls, along with the procedures for using the controls. As the team identifies mitigation strategies, risks may be identified that can be mitigated by "quick fix" solutions-low cost, high value practices that can significantly reduce risk.

Examples of these solutions are restricting Internet access and eliminating e-mail access on operator control stations. Organizations should identify, evaluate, and implement suitable quick fix solutions as soon as possible to reduce security risks and achieve rapid benefits. The Department of Energy provides a 21 Steps to Improve Cyber Security of SCADA Networks document that outlines specific actions to increase the security of SCADA systems and other ICSs.

Providing Training and Security Awareness

Security awareness is a critical part of ICS incident prevention, particularly when it comes to "social engineering" threats. Social engineering is a technique used to manipulate individuals into giving away private information, such as passwords. This information can then be used to compromise otherwise secure systems.

Implementing an ICS security program may bring changes to the way in which personnel access computer programs, applications, and the computer desktop itself.

Organizations should design effective training programs and communication vehicles to help employees understand why new access and control methods are required, ideas they can use to reduce risks, and the impact on the company if control methods are not incorporated. Training programs also demonstrate management's commitment to and value for a cyber security program. Feedback from staff exposed to this type of training can be a valuable source of input for refining the charter and scope of the security program.

Managing Risk

In recognition of the importance of information security to the economic and national security interests of the United States, the [Federal Information Security Management Act \(FISMA\)](#) was established to require each Federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency. [The FISMA Implementation Project](#) [21] was established in January 2003 to produce several key security standards and guidelines required by Congressional legislation to address:

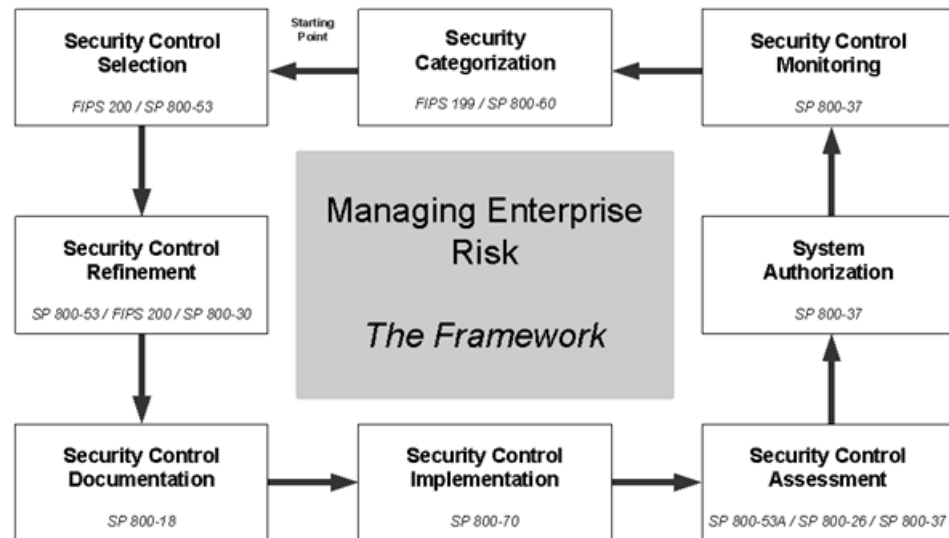
- Standards to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels.
- Guidelines recommending the types of information and information systems to be included in each category.
- Minimum information security requirements (i.e., management, operational, and technical controls) for information and information systems in each category.

The following list of NIST FIPS and Special Publications (SP) documents these standards and guidelines:

- [FIPS Publication 199: Standards for Security Categorization of Federal Information and Information Systems](#) contains standards to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization resulting from the operation of its information systems.
- [FIPS Publication 200: Minimum Security Requirements for Federal Information and Information Systems](#) specifies minimum security requirements for information and information systems supporting the executive agencies of the Federal government and a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements. The document provides links to NIST Special Publication 800-53 (Recommended Security Controls for Federal Information Systems), which recommends management, operational, and technical controls needed to protect the confidentiality, integrity, and availability of all Federal information systems that are not national security systems.
- [NIST SP 800-18, Rev 1: Guide for Developing Security Plans for Information Systems](#) contains guidelines to develop, document, and implement an agency-wide information security program that includes subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems.

- [NIST SP 800-26, Rev 1: Assessment Guide for Information Systems and Security Programs](#) presents guidelines for performing an independent evaluation of the information security program and practices to determine the effectiveness of such programs and practices.
- [NIST SP 800-30: Risk Management Guide for Information Technology Systems](#) has guidelines to develop an agency-wide information security program that includes periodic assessment of the risk and magnitude of the harm that could result from unauthorized access, use disclosure, disruption, modifications, or destruction of information and information systems.
- [NIST SP 800-37: Guide for the Security Certification and Accreditation of Federal Information Systems](#) provides guidance on conducting periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices (including management, operational, and technical security controls).
- [NIST SP 800-53: Recommended Security Controls for Federal Information Systems](#) provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the Federal government. The guidelines apply to all components of an information system that process, store, or transmit Federal information with the exception of systems designated as national security systems. A project is currently underway to provide guidance on the application of SP 800-53 in ICS, including the use of compensating controls to cover control that cannot technically be met in an ICS.
- [NIST SP 800-53A: Guide for Assessing Security Controls in Federal Information Systems](#) provides guidance for conducting periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices (including management, operational, and technical security controls).
- [NIST SP 800-59: Guideline for Identifying an Information System as a National Security System](#) provides guidelines developed in conjunction with the Department of Defense, including the National Security Agency, for identifying an information system as a national security system.
- [NIST SP 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories](#) presents guidelines that recommend the types of information and information systems to be included in each security category defined in FIPS 199.
- [NIST SP 800-70: The NIST Security Configuration Checklists Program](#) discusses the development of security configuration checklists and option selections that minimize the security risks associated with commercial IT products used within the Federal government.

This document set provides security standards and guidelines that support an enterprise-wide risk management process. The documents are intended to be an integral part of a Federal agency's overall information security program. The following graphic shows this framework and the relevancy of supporting documents:



The following is a chronological listing of the Managing Enterprise Risk framework activities, a description of each activity, and identification of supporting NIST documents:

- **Security Categorization:** The first framework activity in the risk management process is to categorize the information system according to potential impact of loss. For each information type and information system under consideration, the three FISMA defined security objectives- confidentiality, integrity, and availability- are associated with one of three levels of potential impact should there be a security breach.

The generalized format for expressing the Security Category (SC) is:

```

SC information type or system =
{ (confidentiality, impact), (integrity, impact),
  (availability, impact) }

```

-- where the acceptable values for potential impact are LOW, MODERATE, or HIGH

The standards and guidance for this categorization process can be found in FIPS 199 and SP 800-60, respectively.

- **Security Control Selection:** This framework activity includes the initial selection of minimum security controls planned or in place to protect the information system based on a set of requirements. FIPS PUB 200 documents a set of minimum security requirements covering 17 security-related areas with regard to protecting the confidentiality, integrity, and availability of Federal information systems and the information process, stored, and transmitted by those systems.

The security-related areas are:

- Access Control (AC)
- Awareness and Training (AT)
- Audit and Accountability (AU)
- Certification, Accreditation, and Security Assessments (CA)
- Configuration Management (CM)

- Contingency Planning (CP)
- Identification and Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Physical and Environmental Protection (PE)
- Planning (PL)
- Personnel Security (PS)
- Risk Assessment (RA)
- System and Services Acquisition (SA)
- System and Communications Protection (SC)
- System and Information Integrity (SI).

To aid in selecting controls to meet these requirements, NIST SP 800-53 provides fundamental concepts and a process for selection and specification of security controls for an information system. Security controls are organized into classes and families for ease of use in the selection and specification process. Each family name and unique control identifier corresponds to the above listing of minimum security requirements. The families are divided among three classes: management, operational, and technical.

Each security control within a family contains the following information:

- **Control:** Describes specific security related activities or actions to be carried out by the organization or the information systems. The control selections often contain assignment and selection options for customizing a security control.
- **Supplemental Guidance:** Provides additional information related to a specific security control that should be considered when selecting security controls.
- **Control Enhancements:** Provide statements of security capability to add functionality to or increase the strength of a basic control.

Security Control Refinement: This activity performs a risk assessment to adjust minimum security controls to local conditions, required threat coverage, and specific agency requirements. NIST SP 800-30 provides practical guidance for assessing and mitigating risks identified within IT systems.

Security Control Documentations: This activity develops a system security plan that provides an overview of the security requirements for the information system and documents the security controls planned or in place. The system security plan also delineates responsibilities and expected behavior of all individuals who access the systems. NIST 800-18 provides a set of activities and concepts for developing an information security plan.

Security Control Implementations: This framework activity involves the implementation of security controls in new or legacy information systems. To help make this process consistent across the Federal government, NIST is currently working to develop security checklists, which are documented sets of instructions for configuring products to pre-defined security baselines.

For an example of a security configuration checklist, see [NIST SP 800-68, Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist](#).

Security Control Assessment: This framework activity determines the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. SP 800-26 helps standardize the system security assessment process by serving as the assessment reporting for the:

- FISMA annual assessment for major information systems.
- Certification documentation.
- Continuous monitoring of selected security controls.
- Preparation for an audit.
- Identification of resource needs to improve the system's security posture.

SP 800-53A provides guidance for assessing security controls initially selected from SP 800-53 to ensure they are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the system. To accomplish this, the document provides expectations based on assurance requirements defined in SP 800-53 for characterizing the expectations of security assessments by impact level.

System Authorization: This activity results in a management decision to authorize the operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls. SP 800-37 provides certification and accreditation guidance in support of this activity.

Security Control Monitoring: This activity continuously tracks changes to the information system that may affect security controls and assesses control effectiveness. SP 800-37 provides guidance of implementing this continuous monitoring.

Creating ICS Security Controls

Security controls prescribe the management, operational, and technical controls (i.e., safeguards or countermeasures) for an informational system to protect the confidentiality, integrity, and availability of the system and its information. This section discusses the security controls specified in **NIST SP 800-53**, which was developed as part of the FISMA implementation project.

NIST SP 800-53 provides guidelines for selecting and specifying security controls for information systems in support of Federal government information systems. Security controls are organized into three classes; management, operational, technical controls. Each class is broken into several families where a family control contains a definition of the control, supplemental guidance, and possible enhancements that will increase the strength of a basic control.

A single security product or technology cannot adequately protect an ICS. Securing an ICS is based on a combination of effective security policies and a properly configured set of security controls. An effective cyber-security strategy for an ICS should apply defense in depth, a technique of layering security mechanisms so that the impact of a failure in any one mechanism is minimized. Use of such a strategy is explored within the security control discussions and their application to ICS that follow.

Management Controls

Management controls determine and define the security countermeasures for an ICS that focus on the management of risk and the management of information security. SP 800-53 defines four families of controls within the Management controls class. These include:

- **Risk Assessment (RA)** - the process of identifying risks to operations, assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact.
- **Developing the Security Plan (PL)** - development and maintenance of a plan to address information system security by performing assessments, specifying and implementing security controls, assigning security levels, and responding to attacks.
- **System and Services Acquisition Procedures (SA)** - allocation of resources for information system security to be maintained throughout the systems life cycle and the development of acquisition policies based on risk assessment results including requirements, design criteria, test procedures, and associated documentation.
- **Certification, Accreditation and Security Assessments (CA)** - assurance that the specified controls are implemented correctly, operating as intended, and producing the desired outcome.

These management controls are discussed in more detail in the following sections.

Risk Assessment (RA)

Risk is a function of the likelihood that a given threat source exercises a potential vulnerability and the resulting impact of this attack on the organization. Risk assessment is the process of identifying risks to an organizations operations, assets, and individuals by determining the probability of occurrence and resulting impacts of a threat. Also included in the assessment is an evaluation of security controls that can mitigate each threat and the costs associated with implementing them.

Risk is a function of probability and consequence. Achieving an acceptable level of risk is a process of reducing the probability of a successful attack that is accomplished by mitigating or eliminating vulnerabilities that can be exploited by an attacker as well as consequences resulting from a successful attack.

Prioritization of vulnerabilities must be based on cost and benefit with the objective of providing a business case for implementing (at least) a minimum set of control system security requirements to reduce risk to an acceptable level. This risk model must also assess the cost of security with the costs associated with successful attacks.

A risk measurement must be determined for each vulnerability selected for mitigation or elimination. A mistake often made during a risk assessment is to select technically interesting vulnerabilities without taking into account the level of risk associated with them. Vulnerabilities should be assessed and rated for risk before trying select and implement security controls on them.

The security controls that fall within the NIST 800-53 Risk Assessment Controls (RA) family provide policy and procedures to develop, distribute and maintain a documented risk assessment policy that describes the purpose, scope, roles, responsibilities and compliance as well as policy implementation procedures. An information system and associated data is categorized base on the security objectives and a range of risk levels. A risk assessment is performed to identify risks and the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of an information system and data. Also included in these controls are mechanisms for keeping risk assessments up-to-date and performing periodic vulnerability scanning.

NIST SP 800-30, Risk Management Guide for Information Technology Systems, provides a risk assessment methodology, which includes the following steps:

1. System characterization - produces a good picture of the information system environment, and delineation of system boundary.
2. Threat identification - produces a threat statement containing a list of threat-sources that could exploit system vulnerabilities.
3. Vulnerability identification - produces a list of the system vulnerabilities that could be exercised by the potential threat sources.
4. Control analysis - produces a list of the planned controls used for the information system to mitigate the likelihood of a vulnerability being exercised and reduce the impact of such an adverse event.
5. Likelihood determination - produces a likelihood rating (High, Medium, or Low) that indicates the probability that a potential vulnerability may be exercised.
6. Impact analysis - produces a magnitude of impact (High, Medium, or Low) resulting from a successful threat exercise of a vulnerability.
7. Risk determination - produces measurement for risk based on a scale of high, medium, or low.
8. Control recommendations - produces recommendations of security controls and alternative solutions to mitigate risk.
9. Results documentation - produces a risk assessment report that describes the threats and vulnerabilities, measures the risk, and provides recommendations for control implementation.

Supplemental guidance for the RA controls can be found in the following documents:

- [800-12](#) provides guidance on security policies and procedures.
- [SP 800-30](#) provides guidance on conducting risk assessments and updates.
- [SP 800-40](#) provides guidance on handling security patches.
- [SP 800-42](#) provides guidance on network security testing.
- [SP 800-60](#) provides guidance on determining the security categories of information types.

FIPS 199 specifies that information systems be categorized as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability.

Definitions for low, moderate, and high levels of security based on impact for ICS are provided in the following table:

Impact Category	Low	Medium	High
Product Controlled	<ul style="list-style-type: none"> • Non-hazardous materials or products • Non-ingested consumer products 	<ul style="list-style-type: none"> • Some hazardous products or steps during production • High amount of proprietary information 	<ul style="list-style-type: none"> • Critical infrastructure • Hazardous materials • Ingested products
Industry Examples	<ul style="list-style-type: none"> • Plastic injection molding • Warehouse applications 	<ul style="list-style-type: none"> • Automotive metal industries • Pulp and paper • Semiconductors 	<ul style="list-style-type: none"> • Utilities • Petrochemical • Food and beverage • Pharmaceutical
Security Concerns	<ul style="list-style-type: none"> • Protecting human life • Capital investment • Ensuring uptime 	<ul style="list-style-type: none"> • Protecting human life • Trade secrets • Capital investment • Ensuring uptime 	<ul style="list-style-type: none"> • Protecting human life • Ensuring basic social services

[ISA-TR99.00.02](#) uses a similar impact level scale which is shown in the following table:

Impact Category	Low	Medium	High
Injury	Cuts, bruises requiring first aid	Requires hospitalization	Loss of life or limb
Financial Loss	\$1,000	\$100,000	\$Millions
Environmental Release	Temporary damage	Lasting damage	Permanent damage, off-site damage
Interruption of Production	Minutes	Days	Weeks
Public Image	Temporary Damage	Lasting Damage	Permanent Damage

Organizations must consider the potential consequences resulting from an attack on an ICS vulnerability. Well-defined policy and procedures lead to mitigation techniques designed to thwart attacks, managing the risk to eliminate or minimize the consequences. The degradation of the physical plant, economic status, or national confidence could all justify mitigation.

A very important aspect of the ICS risk assessment is to determine the value of the data that flows from the control network to the enterprise network. In instances where pricing decisions are determined from this data, the data has a very high value. The fiscal justification for mitigation has to be derived by the cost benefit compared to the effects of the consequence.

It is not possible to define a one-size-fits-all set of security requirements. A very high level of security may be achievable but undesirable in many situations because of the loss of functionality and other associated costs. A well-thought out security implementation is a balance of risk versus cost. In some situations the risk may be safety, health, or environment-related rather than purely economic. The risk may have an unrecoverable consequence rather than a temporary financial setback.

Developing the Security Plan (PL)

A security plan is a formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements. The security controls that fall within the NIST 800-53 Planning Controls (PL) family provide the basis for developing a security plan. These controls also address maintenance issues for periodically updating a security plan.

A set of rules must be specified to describe user responsibilities and expected behavior regarding information system usage with provision for signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior before authorizing access to the information system.

A security plan for an ICS should build on existing IT security experience, programs, and practices. However, there are critical operational differences between IT and ICS that will influence how this security will be applied. A forward-looking plan is needed to provide a method for continuous security improvements.

Cyber-security for ICS is a rapidly evolving field requiring the security planning process to constantly explore emerging ICS security capabilities as well as new threats that are identified by organizations such as the US Computer Emergency Readiness Team (CERT) Control Systems Security Center (CSSC).

Supplemental guidance for the SA controls can be found in the following documents:

- SP 800-12 provides guidance on security policies and procedures.
- SP 800-18 provides guidance on preparing rules of behavior.

System and Services Acquisition Procedures (SA)

The security controls that fall within the NIST 800-53 System and Services Acquisition (SA) family provide the basis for developing policies and procedures for acquiring resources required to adequately protect an information system. These acquisitions are based on security requirements and/or security specifications.

As part of the acquisition procedures, an information system is managed using a system development life cycle methodology that includes information security considerations. As part of acquisition, adequate documentation must be maintained on the information system and constituent components.

The SA family also addresses out sourced systems and the inclusion of adequate security controls by vendors as specified by the supported organization. Vendors are also responsible for configuration management and security testing for these out sourced information systems.

Supplemental guidance for the SA controls can be found in the following documents:

- [SP 800-12](#) provides guidance on security policies and procedures.
- [SP 800-23](#) provides guidance on the acquisition and use of tested/evaluated information technology products.
- [SP 800-27](#) provides guidance on engineering principles for information system security.
- [SP 800-35](#) provides guidance on information technology security services.
- [SP 800-36](#) provides guidance on the selection of information security products.
- [SP 800-64](#) provides guidance on security considerations in the system development life cycle.
- [SP 800-65](#) provides guidance on integrating security into the capital planning and investment control process.
- [SP 800-70](#) provides guidance on configuration settings for information technology products.

In support of the acquisition of secured ICS, the Process Control Security Requirements Forum (PCSRF), an industry-based effort being lead by NIST, has documented a [cohesive, cross-industry set of requirements for new ICS](#) with follow-up work addressing SCADA and subcomponent level requirements.

Note A project started at the SANS 2006 Process Control and SCADA Security Summit is developing a procurement language for specifying security requirements.

The security requirements of an organization outsourcing the management and control of all or some of its information systems, networks, and desktop environments should be addressed in a contract agreed between the parties. External suppliers that have an impact on the security of the organization must be held to the same security policies and procedures to maintain the overall level of ICS security.

Security policies and procedures of second and third-tier suppliers should also be in compliance with corporate cyber security policies and procedures in the case that they impact ICS security.

Certification, Accreditation and Security Assessments (CA)

The security controls that fall within the NIST 800-53 Certification, Accreditation and Assessments (CA) family provide the basis for performing periodic assessments and providing certification of the security controls implemented in the information system to determine if the controls are implemented correctly, operating as intended, and producing the desired outcome in order to meet the system security requirements.

This assessment should also include all connections from the information system to other information systems. A senior organizational official should be responsible for approving the security accreditations.

In addition, all security controls should be monitored on an ongoing basis. Monitoring activities include configuration management and control of information system components, security impact analysis of changes to the system, ongoing assessment of security controls, and status reporting.

Supplemental guidance for the CA controls can be found in the following documents:

- [SP 800-12](#) provides guidance on security policies and procedures.
- [SP 800-26](#) & [800-53A](#) provide guidance on security control assessments.
- [SP 800-37](#) provides guidance on security certification and accreditation.

Operational Controls

Operational controls are the security countermeasures for an ICS that are primarily implemented and executed by people as opposed to systems. SP 800-53 defines nine families of controls within the Operational controls class. These include:

- **Personnel Security (PS)** - Policy and procedures for personnel position categorization, screening, transfer, penalty, and termination. Also addresses third-party personnel security
- **Physical and Environmental Protection (PE)** - Policy addressing physical, transmission, and display access control as well as environmental controls for conditioning (i.e., temperature, humidity) and emergency provisions (i.e., shutdown, power, lighting, fire protection).

- **Contingency Planning (CP)** - Policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.
- **Configuration Management (CM)** - Policy and procedures for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation.
- **Maintenance (MA)** - Policies and procedures to manage all maintenance aspects of an information system.
- **System and Information Integrity (SI)** - Policy and procedures to protect information systems and their data from design flaws and data modification using functionality verification, data integrity checking, intrusions detection, malicious code detection and security alert and advisory controls.
- **Media Protection (MP)** - Policy and procedures to insure secure handling of media. Controls cover access, labeling, storage, transport, sanitization, destruction, and disposal.
- **Incident Response (IR)** - Policy and procedures pertaining to incident response training, testing, handling, monitoring, reporting, and support services.
- **Awareness and Training (AT)** - policies and procedures to ensure that all information system users are given appropriate security training relative to their usage of the system and that accurate training records are maintained.

Personnel Security

The security controls that fall within the NIST 800-53 Personnel Security (PS) family provide policy and procedures to reduce the risk of human error, theft, fraud, or other intentional or unintentional misuse of information systems.

Positions should be categorized with a risk designation and screening criteria and individuals filling a position should be screened against this criteria as well as complete an access agreement before being granted access to an information system.

Supplemental guidance for the PS controls can be found in the following documents:

- [SP 800-12](#) provides guidance on security policies and procedures.
- [SP 800-35](#) provides guidance on information technology security services.
- [SP 800-73](#) provides guidance on interfaces for personal identity verification.
- [SP 800-76](#) provides guidance on biometrics for personal identity verification.

Personnel security measures are meant to reduce the possibility and risk of human error, theft, fraud, or other intentional or unintentional misuse of informational assets. There are three main aspects to personnel security:

- **Hiring Policies:** This includes pre-employment screening, the interview process, hiring policies, complete job descriptions and detailing of duties, terms and condition of employment, and legal rights and responsibilities of employees or contractors.
- **Company Policies and Practices:** These include security policies, information classification, document and media maintenance and handling policies, user training, acceptable usage policies for company assets, periodic employee performance reviews, and any other policies and actions that detail expected and required behavior of company employees, contractors, and visitors.

Company policies to be enforced should be written down and readily available to all workers through an employee handbook, distributed as email notices, located in a centralized resource area, or posted directly at a worker's area of responsibility.

- **Terms and Conditions of Employment:** This category includes job and position responsibilities, notification to employees of terminable offenses, disciplinary actions and punishments, and periodic employee performance reviews.

Protecting the Physical Environment

Security controls that fall within the NIST 800-53 Physical and Environmental (PE) family provide policy and procedures for all physical access to an information system including designated entry/exit points, transmission mediums, and display mediums. These include controls for monitoring physical access, maintaining logs and handling visitors.

This family also includes controls for the deployment and management of emergency protection controls such as emergency shutoff, power, and lighting as well as damage controls such as fire, temperature, humidity and water.

Supplemental guidance for the PE controls can be found in the following documents:

- SP 800-1 provides guidance on security policies and procedures.
- SP 800-46: provides guidance on security in telecommuting and broadband communications.

Physical security measures are designed to reduce the risk of accidental or deliberate loss or damage to plant assets and the surrounding environment. The assets being safeguarded may be physical assets such as tools and plant equipment, intellectual property including proprietary data such as process settings and customer information, the environment, and the surrounding community.

The deployment of physical security controls is often subject to environmental, safety, regulatory, legal, and other requirements that must be identified and addressed specific to a given environment. The subject of deploying physical security controls is vast and needs to be specific to the type of required protection.

The physical protection of the cyber components and data associated with the control system must be addressed as part of the overall security of a plant. Security at many ICS facilities is intimately tied to plant safety. A primary goal is to keep people out of hazardous situations without preventing them from doing their job or carrying out emergency procedures.

A defense-in-depth solution to physical security should include the following attributes:

- **Access Control:** Access control systems must ensure that only authorized people have access to controlled spaces. An access control system must be flexible. The need for access may be based on time (day vs. night shift), level of training, employment status, work assignment, plant status, and a myriad of other factors.

A system must be able to verify that persons being granted access are who they say they are (usually using something the person has, such as an access card; something they know, such as a personal identification number; or something they are, using biometrics).

Access control must be highly reliable, yet not interfere with the routine duties of plant personnel. Integration of access control into the process system allows a view into not only security access, but also physical and personnel asset tracking, dramatically accelerating response time in emergencies, helping to direct individuals to safe locations, and improving overall productivity.

- **People and Asset Tracking:** Locating people and vehicles in a large installation is important for safety reasons, and it is increasingly important for security reasons as well. Asset location technologies can be used to track the movements of people and vehicles within the plant, to ensure that they stay in authorized areas, to identify personnel needing assistance, and to support emergency response.
- **Video surveillance**
- **Intrusion detection**
- **Secure communication**
- **Lighting**
- **Site vulnerability assessments**

Further information regarding physical asset defense-in-depth security can be found in NIST standards located in Appendix A.

Physical Access

Gaining physical access to a control room or control system components often implies gaining logical access to the process control system as well. Likewise, having logical access to systems such as main servers and control room computers allows an attacker to exercise control over the physical process.

If computers are readily accessible, and they have a floppy disk or CD drive, the drives can be fitted with locks or removed from the computers. Depending on security needs and risks, it might also be prudent to disable or physically protect power buttons to prevent unauthorized use.

For maximum security, servers should be placed in locked areas and authentication mechanisms (such as keys) protected. The network devices on the process control network, including switches, routers, network jacks, servers, workstations, and controllers, should be located in a secured area that can only be accessed by authorized personnel. The secured area should also be compatible with the environmental requirements of the devices.

Include environmental factors in security requirements. For example, if a site is dusty, systems should be placed in a filtered environment. This is particularly important if the dust is likely to be conductive or magnetic, as in the case of sites that process coal or iron.

If vibration is likely to be a problem, systems should be mounted on rubber to prevent disk crashes and wiring connection problems. The environments containing systems and media (e.g., backup tapes, floppy disks) should have stable temperature and humidity. An alarm to the process control system should be generated when environmental specifications such as temperature and humidity are exceeded.

Heating, ventilation, and air conditioning (HVAC) systems for control rooms must support plant personnel during emergencies which could include the release of toxic substances. Fire systems must be carefully designed to avoid causing more harm than good (e.g., to avoid mixing water with incompatible products). HVAC and fire systems have significantly increased roles in security that arise from the interdependence of process control and security. For example, fire systems need to be defended from focused terrorist attacks, and HVAC systems that support process control computers need to be defended against cyber attacks.

Reliable power is essential, so an uninterruptible power supply (UPS) should be provided. If the site has an emergency generator, the UPS battery life may only need to be a few seconds; however, if the site relies on external power, the UPS probably needs several hours' supply.

Control Center

Providing physical security for the control room is essential to reduce the potency of many threats. Control rooms frequently have consoles continuously logged onto the primary control server, with speed of response and continual view of the plant considered more important than secure access.

This area will also often contain the servers themselves, other critical computer nodes, and plant controllers. It is essential to limit who can enter this area using authentication methods such as smart or magnetic identity cards or biometric readers.

In extreme cases, it may be considered necessary to make the control room blast-proof, or to provide a second off-site emergency control room so that control can be maintained if the primary area becomes uninhabitable.

Other Asset considerations include Field devices, Portable devices, and Cabling.

Cabling for the control network should be addressed in the cyber-security plan. Unshielded twisted pair cable, while acceptable for the office environment, is generally not suitable for the plant environment due to its susceptibility to interference from magnetic fields, radio waves, temperature extremes, moisture, dust, and vibration.

Industrial RJ-45 connectors should be used because the standard connectors are not water- or dust-tight. Fiber-optic cable is a better choice for the control network and is immune to many of the typical environmental conditions found in an industrial control environment. Typical connectors provide good moisture, dust, and vibration tolerance. Coaxial cable is also acceptable for the plant floor. The shielding protects against electrical interference and the connectors are designed to help protect against vibration, dust, and moisture.

Cable runs should be installed so that access is minimized and equipment installed in locked cabinets with adequate ventilation and air filtration.

Contingency Planning

Contingency plans are management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster. The security controls that fall within the NIST 800-53 Contingency Planning (CP) family provide policy and procedures to implement a contingency plan by specifying roles and responsibilities, assigning personnel and activities associated with restoring the information system after a disruption or failure.

Along with planning, controls also exist for contingency training, testing and plan update and for backup information processing and storage sites.

Supplemental guidance for the CP controls can be found in the following documents:

- [SP 800-12](#) provides guidance on security policies and procedures.
- [SP 800-34](#) provides guidance on contingency planning.

Contingency plans cover the full range of failures or problems that could be caused by failures in the ICS cyber security program. Contingency plans should include procedures for restoring systems from known good backups, separating systems from all non-essential interferences and connections that could permit cyber security intrusions, and alternatives to achieve necessary interfaces and coordination.

Contingency plans should be periodically tested to ensure that they continue to meet their objectives. Organizations also have business continuity plans and disaster recovery plans that are closely related to contingency plans. Because business continuity and disaster recovery plans are particularly important for ICSs, they are described in the following sections.

Planning for Business Continuity

Business continuity planning addresses the overall issue of maintaining or reestablishing production in the case of an undesirable interruption. These interruptions may take the form of a natural disaster (e.g., hurricane, tornado, earthquake, flood), an unintentional man-made event (e.g., accidental equipment damage, fire or explosion, operator error), an intentional man-made event e.g., attack by bomb, firearm or vandalism, hacker or virus) or an equipment failure.

From a potential outage perspective, this may involve typical time spans of days, weeks, or months to recover from a natural disaster to minutes or hours to recover from many mechanical failures. Since there is often a separate discipline that deals with reliability and electrical/mechanical maintenance, some organizations choose to define business continuity in a way that excludes these sources of failure.

Since business continuity also deals primarily with the long-term implications of production outages, some organizations also choose to place a minimum interruption limit on the risks to be considered. For the purposes of ICS cybersecurity, it is recommended that neither of these constraints be made. Long-term outages (disaster recovery) and short-term outages (operational recovery) should both be considered.

Due to the fact that some of these potential interruptions involve man-made events, it is also important to work collaboratively with the physical security organization to understand the relative risks of these events and the physical security countermeasures that are in place to prevent them.

The physical security organization needs to understand which areas of a production site house data acquisition and control systems that might pose higher level risks.

Prior to creating a plan to deal with potential outages, it is important to specify the recovery objectives for the various systems and subsystems involved based on typical business needs. Two distinct types of objectives are necessary: system recovery and data recovery.

System recovery involves the recovery of all communication links and processing capabilities, and it is usually specified in terms of a Recovery Time Objective (RTO). This is defined as the time required to recover all communication links and processing capabilities.

Data recovery involves the recovery of data describing production or product conditions in the past and is usually specified in terms of a Recovery Point Objective (RPO). This is defined as the longest period of time for which an absence of data can be tolerated.

Once the recovery objectives are defined, a list of potential interruptions should be created and the recovery procedure developed and described. For most of the smaller scale interruptions, repair and replace activities based on a critical spares inventory will prove adequate to meet the recovery objectives. When this is not true, contingency plans need to be developed.

Due to the potential cost of these contingency plans, these should be reviewed with the managers responsible for business continuity planning to verify that they are justified.

Once the recovery procedures are documented, a schedule should be developed to test part or all of the recovery procedures. Often the procedures for a specific subsystem are tested annually and the specific subsystem is rotated so the overall system procedures are eventually tested over a five to ten year period.

Particular attention must be paid to the verification of backups of system configuration data and product or production data. Not only should these be tested when they are produced, but the procedures followed for their storage should also be reviewed on some frequency to verify that the backups are kept in environmental conditions that will not render them unusable and that they are kept in a secure location, where they can be quickly obtained by authorized individuals when needed.

Planning for Disaster Recovery

A Disaster Recovery Plan (**DRP**) is essential to continued availability of the ICS. The disaster recovery plan should include the following items:

- Required response to events or conditions of varying duration and severity that would activate the recovery plan.
- Roles and responsibilities of responders.
- Processes and procedures for the backup and secure storage of information.
- Complete and up-to-date logical network diagram.
- Personnel list for authorized physical and cyber access to the ICS.
- List of personnel to contact in the case of an emergency including ICS vendors, network administrators, ICS support personnel, etc.
- Current configuration information for all components.

The plan should assess how quickly replacement components can be obtained in the case of an emergency. If possible, replacements for hard-to-obtain critical components should be kept in inventory.

A comprehensive backup and restore policy should be defined. This policy should consider the following:

- How quickly data or the system needs to be restored, which will indicate the need for a redundant system, spare offline computer, or valid file system backups.
- How frequently critical data and configurations are changing, which will dictate the frequency and completeness of backups.
- The safe onsite and off-site storage locations of full and incremental backups.
- The safe storage locations of installation media, license keys, and configuration information.
- Who will be responsible for performing, testing, storing, and restoring backups.

Configuration Management Policy

Configuration management policy and procedures are used to control modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation.

The security controls that fall within the NIST 800-53 Configuration Management (CM) family provide policy and procedures for establishing baseline controls for information systems. Controls are also specified for maintaining, monitoring and documenting configurations control changes. Access to configuration settings and security settings of information technology products should be set to the most restrictive mode, consistent with information system operational requirements.

Supplemental guidance for the CM controls can be found in the following documents:

- [SP 800-12](#) provides guidance on security policies and procedures.
- [SP 800-70](#): provides guidance on configuration settings for information technology products.

A formal Configuration Change Management procedure is vital for ensuring that any modifications to an ICS control network meet the same security requirements as the components that were included in the original asset evaluation and the associated risk assessment and mitigation plans.

Risk assessment should be performed on any change to the process control network that could affect security, including configuration changes, the addition of network components and installation of software. Changes to policies and procedures might also be required. The ICS control network configuration must always be known.

Maintenance

The security controls that fall within the NIST 800-53 Maintenance (MA) family provide policy and procedure for performing routine and preventative maintenance on the components of an information system.

This includes the usage of maintenance tools (both local and remote) and management of maintenance personnel.

Supplemental guidance for the MA controls can be found in the following documents:

- [SP 800-12](#) provides guidance on security policies and procedures.
- [SP 800-63](#) provides guidance on electronic authentication for remote maintenance.

Maintaining System and Information Integrity

Maintaining system and information integrity assures that sensitive data has not been modified or deleted in an unauthorized and undetected manner.

The security controls that fall within the NIST 800-53 System and Information Integrity (SI) family provide policy and procedure for identifying, reporting, and correcting information system flaws. Controls exist for malicious code detection, spam and spyware protection and intrusion detection tools and techniques. Also provided are controls for receiving security alerts and advisories, and the verification of security functions on the information system.

Controls within this family can detect and protect against unauthorized changes to software and data, provide restrictions to data input and output, and check for the accuracy, completeness and validity of data, as well as handle error conditions.

Supplemental guidance for the SI controls can be found in the following documents:

- [SP 800-12](#) provides guidance on security policies and procedures.
- [SP 800-40](#) provides guidance on security patch installation.
- [SP 800-31](#) provides guidance on intrusion detection.

Malicious Code Detection

Antivirus products use a software engine to evaluate files on a computer's storage devices against an inventory of virus signature files. If one of the files on a computer matches the profile of a known virus, the file is quarantined by the antivirus software so it cannot infect other files or communicate across a network to infect other files on other computers.

A number of vendors that make antivirus software and most control system vendors have certified several products for use with their control systems. To be effective, the antivirus vendor must publish new virus signature files as soon as a new virus is discovered, and these new virus signature files must be downloaded immediately to all the computers that need to be protected.

In general, the antivirus vendors publish the signature files within hours of new viruses being detected, but disseminating the signature files rapidly can be problematic.

ICS vendors should certify the signature within 7 days. Intermediate protection on an ICS network can be obtained by deploying the signature file on the Gateway device (Boundary Installation) as soon as the signature file is available and then deploy the signature file on the ICS equipment after it has been certified by the vendor.

Antivirus tools only function effectively when installed, configured, running full-time, and maintained properly against the state of known attack methods and payloads.

While antivirus tools are common security practice in IT computer systems, their use with an ICS may require adopting special practices including compatibility checks, change management issues, and performance impact metrics.

Antivirus tools may be deployed in three modes:

- **Workstation Installation:** The software is installed and running on a workstation to protect it against network or server-borne attacks and also protect the network and servers from entry of a virus from direct infection of the client from a floppy or other removable media.
- **Server Installation:** The software is installed and running on a shared server to protect against attacks that may attempt to use the access by clients on that server to propagate rapidly.
- **Boundary Installation:** The software is installed at the logical or physical boundaries of a network or system to protect specifically against attacks propagating into or out of the network (i.e., embedded in a DMZ, firewall, or proxy server).

Another complicating issue with antivirus products is the effect they have on computer resources.

Antivirus products have two basic scopes of operation: total system and incremental. Typically, a total system scan is performed when the antivirus product is initially installed to identify and quarantine any viruses that may already be present. Once the antivirus product is installed, it is set to only scan files that are added incrementally.

A total system scan will typically use most of a system's CPU resources, which is not an issue when the system is undergoing initial configuration and is not being used to control a process. If this is attempted while control applications are being used, the control application will commonly be starved for resources and will not update at the desired frequency. This can at least cause loss of operator view and at worst cause faulty operation.

Some major ICS vendors recommend or support the use of particular antivirus tools. In some cases, control system vendors may have performed regression testing across their product line for supported versions of a particular antivirus tool and also provide associated installation and configuration documentation. Efforts are underway to develop a general set of guidelines and test procedures focused on ICS performance impacts to fill the gaps where ICS and antivirus vendor guidance is not available.

Major antivirus vendors release software patches to upgrade detection and isolation of a new attack within hours. The management of upgrading the virus signatures and virus scanning algorithms require importing information, either by the Internet or by removable media. Importing information may conflict with security policies and procedures to control change management and isolation of the ICS network, either physically or by firewall, from business systems and the Internet at large.

Additionally, consideration of performance impacts on the ICS must be considered during upgrades as well as during the selection of scanning algorithms based on risk of infection. Performance degradation on any one ICS component could affect the performance of the overall ICS.

Intrusion Detection and Prevention

Intrusion detection systems (**IDS**) monitor either traffic patterns on the network or files in host computers, looking for signs and generating alarms that indicate an intruder has or is attempting to break into a system. These systems ensure that unusual activity (such as new open ports, unusual traffic patterns, or changes to critical operating system files) is brought to the attention of the appropriate security personnel.

The two most commonly used types of IDS are:

- **Network-Based IDS:** These systems monitor network traffic and generate alarms when they identify traffic that they deem to be an attack.
- **Host-Based IDS:** Software that monitors a system or application log files. These systems respond with an alarm or countermeasure when a user attempts to gain access to unauthorized data, files, or services.

An effective IDS deployment typically involves both host-based and network-based IDS. In the ICS environment, network-based IDS are most often deployed between the control network and the enterprise network in conjunction with a firewall; host-based IDS are most often deployed on the computers that use general-purpose OSs or applications. Properly configured, an IDS can greatly enhance the security management team's ability to detect attacks entering or leaving the system, thereby improving security. They can also potentially improve a control network's efficiency by detecting non-essential traffic on the network. However, even when intrusion detection systems are implemented, security staff can primarily recognize individual attacks, as opposed to organized patterns of attacks over time.

Managing Patches

Policies regarding applying patches to OS components create another situation where standard IT procedures do not fit the ICS environment.

A patch may remove a vulnerability, but it can also introduce a greater risk from a production or safety perspective. Patching the vulnerability may also change the way the OS or application works with control applications, causing the control application to lose some of its functions. A threat assessment process should be used to evaluate when it is most cost-effective to deploy a security patch.

To conduct that threat assessment, it is important to know how many instances of the target application are in use and where they are. There are tools that allow this type of information to be gathered automatically from a centralized location. Once the decision is made to deploy a patch, there are other tools that automate this process from a centralized location and then confirm that the patch has been deployed correctly.

Media Protection

The security controls that fall within the NIST 800-53 Media Protection (MP) family provide policy and procedures for limiting the access to media to authorized users. Controls also exist for labeling media for distribution and handling requirements, as well as storage, transport, sanitization (removal of information from digital media), destruction and disposal of the media.

Supplemental guidance for the MP controls can be found in the following documents:

- [SP 800-12](#) provides guidance on security policies and procedures.
- [SP 800-36](#) provides guidance on appropriate sanitization equipment, techniques and procedures.

Media assets include compact discs (CD), printed reports, and documents. Physical security controls should address specific requirements for the safe maintenance of these assets and provide specific guidance for transporting, handling, and destroying these assets.

Security requirements could include safe storage from fire, theft, unintentional distribution, or environmental damage. If an attacker gains access to backup media associated with a control system, it could provide valuable data for launching an attack. Recovering an authentication file from the backups might allow an attacker to run password cracking tools and extract usable passwords. In addition, the backups typically contain machine names, IP addresses, software version numbers, usernames, and other data useful in planning an attack.

The use of any unauthorized CDs, DVDs, floppy disks, USB memory sticks, or similar removable media on any node that is part of or connected to the ICS must not be permitted to prevent the introduction of malware or the inadvertent loss or theft of data.

Incident Response

An incident response plan is a documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization's information systems(s). The security controls that fall within the NIST 800-53 Incident Response (IR) family provide policy and procedures for incident response monitoring, handling and reporting.

The handling of a security incident includes preparation, detection, and analysis, containment, eradication, and recovery. Controls also cover incident response training for personnel and testing incident response capability for an information system.

Supplemental guidance for the IR controls can be found in the following documents:

- [SP 800-12](#) provides guidance on security policies and procedures.
- [SP 800-61](#): provides guidance on incident handling and reporting.

Regardless of the steps taken to protect an ICS, it is always possible that it may be compromised by an intrusion. The following symptoms can arise from normal network problems, but when several symptoms start to appear, a pattern may indicate the ICS is under attack and may be worth investigating further.

Note If the attacker is skilled, it may not be obvious that an attack is underway.

The symptoms of an attack could include any of the following:

- Unusually heavy network traffic.
- Out of disk space or significantly reduced free disk space.
- Unusually high CPU usage.
- Creation of new user accounts.
- Attempted or actual use of administrator-level accounts.
- Locked-out accounts.
- Account in use when the user is not at work.
- Cleared log files.
- Full log files with unusually large number of events.
- Antivirus or intrusion detection system alerts.
- Disabled antivirus software and other security controls.
- Unexpected patch changes.
- Machines connecting to outside IP addresses.
- Requests for information about the system (social engineering attempts).
- Unexpected changes in machine configuration settings.
- Unintentional machine shutdown.

Incident response planning defines procedures to be followed when an intrusion occurs. Planning a response minimizes the effects of these intrusions. NIST SP 800-61, Computer Security Incident Handling Guide, provides guidance on incident response planning, might include the following items:

- **Classification of Incidents:** The various types of incidents that might be caused by system intrusion should be identified and classified as to effects and likelihood so that a proper response can be formulated for each potential incident.
- **Response Actions:** Various responses are possible in the event of a system intrusion. These range from doing nothing to full system shutdown. The response taken will depend on the type of incident and its effect on the system.

A written plan documenting the types of incidents and the response to each type should be prepared. The plan provides guidance during times when there might be confusion or stress due to the incident. This plan should include step-by-step actions to be taken by the various organizations.

If there are reporting requirements, these should be noted as well as where the report should be made and phone numbers to reduce reporting confusion.

- **Recovery Actions:** The results of the intrusion might be minor or could cause many problems in the system. In each case, step-by-step recovery actions should be documented so that the system can be returned to normal operations as quickly and safely as possible.

During the preparation of the incident response plan, input should be obtained from the various stakeholders including Operations, Management, Legal, and Safety operational groups. These stakeholders should also review and approve the plan.

Awareness and Training

The security controls that fall within the NIST 800-53 Awareness and Training (AT) family provide policy and procedures for ensuring that all user of an information system are exposed to basic information system security awareness materials before authorization access is provided.

An organization must identify, document, and train all personnel with significant information system roles and responsibilities. Personnel training must be monitored and documented.

Supplemental guidance for the AT controls can be found in the following documents:

- [SP 800-12](#) provides guidance on security policies and procedures.
- [SP 800-50](#): provides guidance on security awareness training.

Technical Controls

Technical controls are the security countermeasures for an ICS that are primarily implemented and executed by the system through mechanisms contained in the hardware, software, or firmware components of the system.

SP 800-53 defines four families of controls within the Technical controls class. These include:

- **Identification and Authentication (IA)** - The process of verifying the identity of a user, process, or device, as a prerequisite for granting access to resources in an IT system.
- **Access Control (AC)** - The process of granting or denying specific requests for obtaining and using information and related information processing services for physical access to areas within the information system environment.
- **Audit and Accountability (AU)** - Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
- **System and Communications Protection (SC).**

Additional ICS-specific guidance pertaining to technical controls can be found in ISA TR99.00.01 and the EPRI report: Supervisory Control and Data Acquisition (SCADA) Systems Security Guide.

Authentication and Authorization

Authentication describes the process of positively identifying potential network users, hosts, applications, services, and resources using a combination of identification factors or credentials.

The result of this authentication process then becomes the basis for permitting or denying further actions (i.e., when an automatic teller machine asks for a PIN). Based on the response received, the system may or may not allow the potential user access to its resources. Authorization is the process of determining who and what should be allowed to have access to a particular resource, or perform an action. Access control is the mechanism for enforcing authorization.

Several methods are possible for determining the authenticity of a person, device or system. For example, the test could be something known (e.g., PIN number or password), something owned (e.g., key, dongle, smart card), something physical (e.g., biological characteristic such as a fingerprint or retinal signature), a location (e.g., Global Positioning System [GPS] location access), the time a request is made, or a combination of these attributes. In general, the more factors that are used in the authentication process, the more robust the process will be.

Note When two or more factors are used, the process is known generically as multi-factor authentication.

The security controls that fall within the NIST 800-53 Identification and Authentication (IA) family provide policy and guidance for the identification and authentication of users-of and devices-within the information system. These include controls to manage identifiers and authenticators within each technology used (i.e., tokens, certificates, biometrics, passwords, keycards).

- [SP 800-12](#) provides guidance on security policies and procedures.
- [SP 800-63](#) provides guidance on remote electronic authentication.
- [SP 800-73](#) provides guidance on interfaces for personal identity verification.
- [SP 800-76](#) provides guidance on biometrics for personal identity verification.

Computer systems in ICS environments typically rely on traditional passwords for authentication. Control system suppliers often supply systems with default passwords. These passwords are often easy to guess or infrequently changed, which creates additional security risks.

Protocols currently used in ICS environments generally have inadequate or no network service authentication. There are now several forms of authentication available in addition to traditional password techniques being used with ICSs. Some of these, including password authentication, are presented in the following sections with discussions regarding their use with ICSs.

Password Authentication

Password authentication technologies determine authenticity based on testing for something the device or human requesting access should know, such as a PIN number or password. Password authentication schemes are thought of as the simplest and most common forms of authentication.

Password vulnerabilities can be reduced if the vendor implements an active password checker that prohibits weak, recently used, or commonly used passwords. Another weakness is the ease of third-party eavesdropping. Passwords typed at a keypad or keyboard are easily observed or recorded, especially in areas where attackers could plant tiny wireless cameras or keystroke loggers. Network service authentication often transmits passwords as plaintext (unencrypted), allowing any network capture tool to expose the password.

One problem with passwords unique to the ICS environment is that a user's ability to recall and enter a password may be impacted by the stress of the moment. During a major crisis when human intervention is critically required to control the process, an operator may panic and have difficulty remembering or entering the password and either be locked out completely or be delayed in responding to the event. It is recommended not to use password authorizations on these critical control systems but instead to use other compensating controls, such as rigorous physical security controls to meet the password control that cannot technically be met.

Some ICS operating systems make setting secure passwords difficult, as the password size is very small and the system allows only group passwords at each level of access, not individual passwords.

Some industrial (and Internet) protocols transmit passwords in plaintext, making them susceptible to interception. In cases where this practice cannot be avoided, it is important that users have different (and unrelated) passwords for use with encrypted and non-encrypted systems.

The following are general recommendations and considerations with regards to the use of passwords. Specific recommendations are presented in [ISA-TR99.00.02-2004](#).

- Passwords should have appropriate length and entropy characterization for the security required. In particular, they should not be able to be found in a dictionary or contain predictable sequences of numbers or letters.
- Passwords should be used with care on operator interface devices such as control consoles on critical processes. Using passwords on these consoles could introduce potential safety issues if operators are locked out during critical events.
- The keeper of master passwords should be a trusted employee, available during emergencies.
- Authority to change higher-level passwords should be limited to trusted employees. A password log, especially for master passwords, should be maintained separately from the control systems, possibly in a notebook locked in a vault or safe.

- In environments with a high risk of interception or intrusion (such as remote operator interfaces in a facility that lacks local physical security access controls), users should consider supplementing password authentication with other forms of authentication such as challenge/response or two-factor authentication using biometric or physical tokens.
- For user authentication purposes, password use is common and generally acceptable for users logging directly into a local device or computer. Passwords should not be sent across any network unless protected by some form of FIPS approved strong encryption or salted cryptographic hash specifically designed to prevent replay attacks. It is assumed that the device used to enter a password is connected to the network in a secure manner.
- For Network Service Authentication purposes, passwords should be avoided if possible. There are more secure alternatives available, such as challenge/response or public-key authentication.

Challenge/Response Authentication

Challenge/response authentication requires that both the service requester and service provider know a "secret" code in advance.

When service is requested, the service provider sends a random number or string as a challenge to the service requester. The service requester uses the secret code to generate a unique response for the service provider. If the response is as expected, it proves that the service requester has access to the "secret" without ever exposing the secret on the network.

Challenge/response authentication addresses the security vulnerabilities of traditional password authentication. When passwords (hashed or plain) are sent across a network, a portion of the actual "secret" itself is being sent. Authentication is performed by giving the secret to the remote device.

Common challenge/response systems include:

- **Point-to-Point Protocol Challenge Handshake Authentication Protocol (PPP-CHAP):** Defined in Internet Engineering Task Force (IETF) Request for Comments (RFC) 1994, PPP-CHAP allows a remote client to connect over a serial or dial-up link to a server. The client must still know the password, but CHAP uses a challenge/response system to verify the password without sending it across the serial line where an attacker may see or replay it.
- **Kerberos:** Defined in IETF RFC1510, Kerberos is a centralized server system designed for small, single-authority networks. It allows servers to provide service to clients based on a simple, secure "ticket" concept. A theoretical example is an OPC server that obtains a data read ticket from a central Kerberos server and submits it to a PLC before the PLC will answer data requests. Many operating systems, such as versions of Windows and UNIX/Linux, support Kerberos.

For user authentication, the direct use of challenge/response authentication is not feasible.

For network service authentication the use of challenge/response authentication is preferable to more traditional password or source identity authentication schemes.

Physical Token authentication

Physical token authentication is similar to password authentication, except that these technologies determine authenticity by testing for a device or token the person requesting access should have in his/her possession, such as security tokens or smart cards.

Private keys are commonly embedded in physical devices such as USB dongles. Some tokens support single-factor authentication only, so that simply having possession of the token is sufficient for authentication. Others support dual-factor authentication that require knowledge of a PIN or password in addition to possessing the token in order to be authenticated.

The primary vulnerability that token authentication addresses is the ability to prevent the secret from being easily duplicated or shared with others. It eliminates the all-too-common scenario of a password to a "secure" system being left on the wall next to the PC or operator station. The security token cannot be duplicated without special access to equipment and supplies.

A second benefit is that the secret within a physical token can be very large, physically secure, and randomly generated. Because it is embedded in metal or silicon, it does not have the same risks as manually-entered passwords. If a security token is lost or stolen, the authorized user loses access, unlike traditional passwords that can be lost or stolen without notice.

Common forms of physical/token authentications include:

- Traditional physical lock and keys.
- Security cards (e.g., magnetic, smart-chip, optical coding).
- Radio-frequency devices in the form of cards, key fobs, or mounted tags.
- Dongles with secure encryption keys that attach to the USB, serial, or parallel ports of computers.
- One-time-authentication code generators.

For single-factor authentication, the largest weakness is that physically holding the token means access is granted; e.g., anyone finding a set of lost keys now has access to whatever the key(s) open.

Physical/token authentication is more secure when combined with a second form of authentication, such as a memorized PIN used along with the token.

Dual-factor authentication is an accepted good practice for high-security applications.

Physical/token authentication has the potential for a strong role in industrial control systems environments. An access card or other token can be an effective form of authentication for computer access, as long as the computer is in a secure area (i.e., once the operator has gained access to the room with appropriate secondary authentication, the card alone can be used to enable control actions).

Where additional security is warranted, single-factor methods such as passwords can be combined with physical/token authentication to create a significantly more secure two-factor authentication system.

Biometric Authentication

Biometric authentication technologies determine authenticity by determining presumably unique biological characteristics of the human requesting access. Usable biometric features include finger minutiae, facial geometry, retinal and iris signatures, voice patterns, typing patterns, and hand geometry.

Like physical token and smart cards, biometric authentication enhances software-only solutions, such as password authentication, by offering an additional authentication factor and removing the human element in memorizing complex secrets. In addition since biometric characteristics are supposedly unique to a given individual, biometric authentication addresses the issues of lost or stolen physical token and smart cards.

Noted issues with biometric authentication include:

- Distinguishing a real object from a fake (e.g., how to distinguish a real human finger from a silicon-rubber cast of one or a real human voice from a recorded one).
- Generating type-I and type-II errors (the probability of rejecting a valid biometric image, and the probability of accepting an invalid biometric image, respectively). Biometric authentication devices should be configured to the lowest crossover between these two probabilities, also known as the crossover error rate.
- Handling environmental factors such as temperature and humidity to which some biometric devices are sensitive.
- Retaining biometric scanners occasionally "drift" over time. Human biometric traits may also shift over time, necessitating periodic scanner retraining.
- Requiring face-to-face technical support and verification for device training, unlike a password that can be given over a phone or an access card that can be handed out by a receptionist.
- Denying needed access to the control system because of a temporary inability of the sensing device to acknowledge a legitimate user.
- Being socially acceptable. Some biometric authentication devices are considered more acceptable than others by users. For example, retinal scans are very low on the scale of acceptability, while iris scanners and thumb print scanners are high on the scale of acceptability. Users of biometric authentication devices will need to determine the level of social acceptability within the target group when evaluating biometric authentication technologies.

Biometric devices make a useful secondary check, versus other forms of authentication that can become lost or borrowed. Using biometric authentication in combination with token key or badge-operated employee time clocks increases the security level. A possible application is in a control room that is environmentally controlled and physically secured.

Controlling Access

The security controls that fall within the NIST 800-53 Access Control (AC) family provide policy and procedures for specifying the use of system resources by only authorized users, programs, processes, or other systems. The Access Control family provides specific controls for managing information system accounts, including establishment, activating, modifying, reviewing, disabling, and removing accounts.

Controls cover access and flow enforcement issues such as separation of duties, least privileged user, unsuccessful login attempts, system use notification, previous logon notification, concurrent session control, session lock, and session termination.

There are also controls to address the use of portable and remote devices, and personally-owned information systems to access the information system as well as the use of remote access capabilities and implementation of wireless technologies.

Supplemental guidance for the AC controls can be found in the following documents:

- [SP 800-12](#) provides guidance on security policies and procedures.
- [SP 800-63](#) provides guidance on remote electronic authentication.
- [SP 800-48](#) provides guidance on wireless network security with particular emphasis on the IEEE 802.11b and Bluetooth standards.

Access control technologies are filter- and blocking technologies designed to direct and regulate the flow of information between devices or systems once authorization has been determined.

The following sections present several access control technologies and their use with ICS.

Role Based Access control

Role based access control (RBAC) is a technology that has the potential to reduce the complexity and cost of security administration in networks with large numbers of intelligent devices. Under RBAC, security administration is simplified by using roles, hierarchies, and constraints to organize user access levels. RBAC reduces costs within an organization because it accepts that employees change more frequently than the duties within positions.

Access can take several forms, including viewing, using, and altering specific data or device functions. The promise of RBAC is a uniform means to manage access to plant floor devices while reducing the cost of maintaining individual device access levels and minimizing errors.

The traditional approach to controlling access to information and network resources is to establish specific permissions for each user. Permissions are then configured into the security level mechanisms supported by the individual intelligent devices.

An industrial control system may have thousands of devices, including DCSs, HMIs, process historians, PLCs, motor control centers, smart sensors, and application-specific data concentrators. While effective in a static environment, this approach is difficult to manage in dynamic environments where users enter and leave employment and contractors, original equipment manufacturers (OEM), system integrators, and vendors come and go.

The constant stream of changes requires frequent updates to access permissions, a time-consuming and error-prone process. For example, timely permission updates are not always performed, enabling unauthorized users (such as terminated employees) to access restricted functions. Quite often, plants either do not use or simply disable individual device security access levels for this reason.

In the absence of uniform authorization tools, most ICS designers take precautions to minimize the amount of external traffic to and from the control system. Most commonly, various architectural measures insure that data flow is in a one-way direction out of the control system to the other enterprise systems. While RBAC may increase the safety of spontaneous data requests to the control system, it is not a panacea for careless design of the data flows.

Web Servers in the ICS Security Model

Web and Internet technologies are being added to a wide variety of ICS products because they make information more accessible and products more user friendly and easier to configure remotely.

SCADA and historian software vendors typically provide Web servers as a product option so that production information can be accessed by users outside the control room. In many cases, software components known as ActiveX controls or Java applets must be installed or downloaded onto each client machine accessing the Web server. Some products, such as PLCs and other control devices, are available with embedded Web, FTP, and email servers to make them easier to configure remotely and allow them to generate e-mail notifications and reports when certain conditions occur.

Web servers and Internet technologies are attractive because of the features and convenience they add to an ICS installation. However, they also add risks and create new security vulnerabilities that need to be addressed.

Virtual Local Area Network (VLAN)

Virtual Local Area Networks (VLAN) divide physical networks into smaller logical networks to increase performance, improve manageability, and simplify network design. VLANs are achieved through configuration of Ethernet switches. Each VLAN consists of a single broadcast domain that isolates traffic from other VLANs.

Just as replacing hubs with switches reduces collisions, using VLANs limits the broadcast traffic, as well as allowing logical subnets to span multiple physical locations.

There are two categories of VLANs:

- Static, often referred to as port-based, where switch ports are assigned to a VLAN so that it is transparent to the end user.

- Dynamic, where an end device negotiates VLAN characteristics with the switch or determines the VLAN based on the IP or hardware addresses.

Although more than one IP subnet may coexist on the same VLAN, the general recommendation is to use a one-to-one relationship between subnets and VLANs. This practice requires a router or multi-layer switch to join multiple VLANs. Many routers and firewalls support tagged frames so that a single physical interface can be used to route between multiple logical networks.

VLANs are not typically deployed to address host or network vulnerabilities in the way that firewalls or intrusion detection systems are. However, when properly configured, VLANs allow switches to enforce security policies and segregate traffic at the Ethernet layer. Properly-segmented networks can also mitigate the risks of broadcast storms that may result from port scanning or worm activity.

Switches have been susceptible to attacks such as MAC spoofing, table overflows, and attacks against the spanning tree protocols, depending on the device and its configuration. VLAN hopping, the ability for an attack to inject frames to unauthorized ports, has been demonstrated using switch spoofing or double-encapsulated frames. These attacks cannot be conducted remotely and require local physical access to the switch.

A variety of features such as MAC address filtering, port-based authentication using IEEE 802.1x, and specific vendor best practices can be used to mitigate these attacks, depending on the device and implementation.

VLANs have been effectively deployed in plant floor networks with each automation cell assigned to a single VLAN to limit unnecessary traffic flooding and allow network devices on the same VLAN to span multiple switches.

Dial-up Modems

ICS systems have high availability needs. When there is a need to troubleshoot and repair, the technical resources are not physically located at the control room or plant. Therefore, ICS often use modems to allow the vendors or system integrators to dial in to diagnose, repair, configure, and perform maintenance on the network or component. While this allows easy access for approved personnel, if not properly secured they can provide back-door entries for unauthorized abuse.

The following is guidance for dial-up modems on ICSs:

- Consider using callback systems when dial-up modems are installed in an ICS. This ensures that the dialer must already have the phone number from where they will be dialing in a callback database prior to making the call.
- Ensure that strong passwords are in place and that the default password has been changed on each modem.
- If possible, disconnect modems when not in use.

Wireless Access

The use of wireless within an ICS is a risk-based decision that has to be determined by the organization. Generally, wireless LANs should only be deployed where health, safety, environmental and financial implications are Low.

The following is guidance for ICS wireless devices:

- When wireless devices are utilized by the system, a wireless survey should be performed to determine antenna location and strength to minimize exposure of the wireless network.
- Where process control network wireless worker devices are used those devices should at a minimum utilize: IEEE 802.1x authentication with a RADIUS server using PEAP protocol.
- The wireless access points and data servers for wireless worker devices should be located on an isolated network with single-point connection to the process control network topology.
- Wireless access points should be configured to a unique SSID, disable SSID broadcast, enable MAC filtering at a minimum.
- The wireless worker devices if being utilized in a Microsoft Windows process control system should be configured into a separate organizational unit of the Windows domain.
- Wireless worker device communications should be encrypted. This can be accomplished by running a VPN on top of the wireless communication.

Security Auditing and Accountability (AU)

An audit is an independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

The security controls that fall within the NIST 800-53 Audit and Accountability (AU) family provide policy and procedures for generating audit records, their content, capacity, and retention requirements. The controls also provide safeguards to react to the event of an audit failure or if an audit log capacity is reached. Audit data must be protected from modification and be designed with non-repudiation capability.

Supplemental guidance for the AU controls can be found in the following documents:

- [SP 800-12](#) provides guidance on security policies and procedures.
- [SP800-61](#) provides guidance on computer security incident handling and audit log retention.

It is necessary to determine that the system is performing as intended. Periodic audits of the industrial control system should be implemented to validate the following items:

- The security controls present during system validation testing are still installed and operating correctly in the production system.

- The production system is free from security compromises and provides information on the nature and extent of compromises, should they occur.
- The management of change program is being rigorously followed with an audit trail of reviews and approvals for all changes.

The results from each periodic audit should be expressed in the form of performance against a set of predefined and appropriate metrics to display security performance and security trends. Security performance metrics should be sent to the appropriate stakeholders, along with a view of security performance trends.

The primary basis for audit in IT systems is logging. Using logging tools within an ICS environment requires extensive knowledge from an IT professional familiar with critical production and safety implications for the facility. Many of the process control devices that are integrated into the ICS have been installed for many years and do not have the capability to provide the logs described in this section. Therefore, the applicability of these more modern tools for auditing system and network activity is dependent upon the age of the components in the ICS.

In cases where the log and audit capability exists, the stability of the ICS is a plus to employing managed scripts for auditing and maintenance. The critical tasks in managing a network in an ICS environment are ensuring reliability and availability to support safe operation.

In regulated industries, security and authentication management, registry and installation integrity management, and all functions that can augment an installation and operational qualification exercise add to the complexity of network management in the regulated manufacturing environments. Cautious use of auditing and log management tools can provide valuable assistance in maintaining and proving the integrity of the ICS from installation through the system life cycle. The value of these tools in this environment can be calculated by the effort required to re-qualify or otherwise retest the ICS where the integrity due to attack, accident, or error is in question. The system should provide reliable synchronized time stamps.

System auditing utilities should be incorporated into new and existing ICS projects. The value these tools provide in tangible logs of evidence and system integrity is enough to warrant their use. Additionally, active log management utilities can actually flag an attack or event in progress and provide location and tracing information to help respond to an attack.

System and Communications Protection

Supplemental guidance for the AU controls can be found in the following documents:

- [SP 800-12](#) provides guidance on security policies and procedures.
- [SP 800-28](#) provides guidance on active content and mobile code.
- [SP 800-56](#) provides guidance on cryptographic key establishment.
- [SP 800-57](#) provides guidance on cryptographic key management.
- [SP 800-58](#) provides guidance on security considerations for VOIP technologies.

- [SP 800-63](#) provides guidance on remote electronic authentication.

Encryption

Encryption is the cryptographic transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called "decryption," which is a transformation that restores encrypted data to its original state.

Encryption within an ICS has to be implemented with caution, since encryption slows communications. This is because additional time is required to encrypt, decrypt, and authenticate each message. Encrypted messages are often longer than unencrypted messages due to one or more of the following items:

- Additional check sums to reduce errors.
- Protocols to control the cryptography.
- Padding (for block ciphers).
- Authentication procedures.
- Other required cryptographic processes

Time increases can be in the tens of milliseconds for retrofit link encryptors on slow lines (300 to 19,600 baud) and milliseconds for embedded encryption. Depending on the protocol and system configuration, there may be problems with link encryptors encrypting both the message and the address, making messages impossible to route in a multi-drop configuration. Some systems may not support broadcast or multicast commands.

Encryption security policies also introduce key management issues. Good security policies require periodic key changes. This process becomes more difficult as the geographic size of the process control system increases, with extensive SCADA systems being the most severe example. Because site visits to change keys can be costly and slow, it is useful to be able to change keys remotely.

The most effective safeguard is to use a complete cryptographic system approved by the NIST/ Communications Security Establishment (CSE) Cryptographic Module Validation Program (CMVP).

Standards ensure that cryptographic systems were studied carefully for weaknesses by a wide range of experts, rather than being developed by a few engineers in a single company. At a minimum, certification makes it probable that:

- Some method (such as counter mode) will be used to ensure that the same message does not generate the same value each time.
- ICS messages are protected against replay and forging.
- Key management is secure throughout the life cycle of the key.
- The system is using an effective random number generator.
- The entire system has been implemented securely.

Even then, the technology is only effective if it is an integral part of an effectively enforced information security policy. [American Gas Association \(AGA\) report 12-1](#) contains an example of such a security policy. While it describes a SCADA system, many of its policy recommendations could apply to any ICS.

For an ICS, encryption can be deployed as part of a comprehensive, enforced security policy. Organizations should select cryptographic protection matched to the value of the information being protected and ICS operating constraints. Specifically, a cryptographic key should be long enough so that guessing it or determining it through analysis takes more effort, time, and cost than the value of the protected asset.

The encryption hardware should be protected from physical tampering and uncontrolled electronic connections. Organizations should select encryption protection with remote key management if the units being protected are so numerous or geographically dispersed that changing keys is difficult or expensive.

Virtual Private Network (VPN)

One method of encrypting data is through a virtual private network (VPN), which is a private network that operates as an overlay on a public infrastructure, so that private network can function across a public network. The most common types of VPN technology implemented include:

- **Internet Protocol Security (IPsec):** IPsec is a set of standards defined by IETF to govern the secure communications of data across public networks at the IP layer. IPsec is included in many current operating systems. The intent of the standards are to guarantee inter operability across vendor platforms, however, the reality is that determination of interpretability of multi-vendor implementations depends on specific implementation testing conducted by the end-user organization.

IPsec supports two encryption modes: **Transport** and **Tunnel**. Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. The (more secure) Tunnel mode encrypts both the header and the payload. On the receiving side, an IPsec-compliant device decrypts each packet. The protocol has been continually enhanced that address specific requirements from the market, such as extensions to the protocol to address individual user authentication and network address translation (NAT) device transversal.

These extensions are typically vendor-specific and can lead to inter operability issues primarily in host-to-security gateway environments. NIST SP 800-87 provides guidance on IPsec VPNs.

- **Secure Sockets Layer (SSL):** SSL provides a secure channel between two machines; the channel is oblivious to the data passing over it.

Note The IETF made slight modifications to the SSL version 3 protocol and created a new protocol called Transport Layer Security (TLS). The terms "SSL" and "TLS" are often used interchangeably and this document generically uses the SSL terminology.

SSL is most often recognized for securing HTTP traffic; this protocol implementation is known as HTTP Secure (HTTPS). However, SSL is not limited to HTTP traffic; it can be used to secure many different application layer programs. SSL-based VPN products have gained acceptance because of the market for "clientless" VPN products. These products actually use standard Web browsers as clients, which have built-in SSL support. The "clientless" term means that there is no need to install or configure third-party VPN "client" software on users' systems.

- **Secure Shell (SSH):** SSH is a command interface and protocol for securely gaining access to a remote computer. It is widely used by network administrators to remotely control Web and other types of servers. The latest version, SSH2, is a proposed set of standards from the IETF. Typically, SSH is deployed as a secure alternative to the telnet application. SSH is included in most UNIX distributions, and is typically added to other platforms through a third-party package.

VPNs are most often used in the ICS environment to provide secure access from an untrusted network to the ICS control network. Untrusted networks can range from the Internet to the corporate LAN. Properly configured, VPNs can greatly restrict access to and from control system host computers and controllers, thereby improving security. They can also potentially improve control network responsiveness by removing unauthorized non-essential traffic from the intermediary network.

VPN devices used to protect control systems should be thoroughly tested to verify that the VPN technology is compatible with the application and that the VPN devices do not unacceptably affect traffic characteristics of the implementation.

C H A P T E R 4

Managing Security Patches and Virus Protection

Keeping a Supervisory and Control System secure and reliable will be almost impossible without implementing Security Patch Management practices.

Microsoft defines "Patch Management" as the following:

The term patch management describes the tools, utilities, and processes for keeping computers up to date with new software updates that are developed after a software product is released. Security patch management is a term that is intended to describe patch management with a focus on reducing security vulnerabilities.

- The Microsoft Guide to Security Patch Management

Contents

- Managing Security Patches
- Virus and Malware Protection

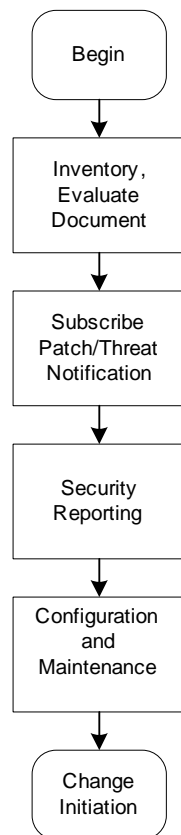
Managing Security Patches

Most software vendors offer tools and utilities that can support a patch management process. However, a process must be defined and implemented in order to take advantage of these tools. A security patch management process should take into account the following:

Setup

Setting up a Security Patch management System requires completing the following tasks:

- Taking Inventory and documenting your system
- Evaluate your security risk and needs
- Subscribing to security alerts and other information sources
- Establishing security reporting to assist with issue identification
- Configuring a patch management system
- Maintaining the patch management system

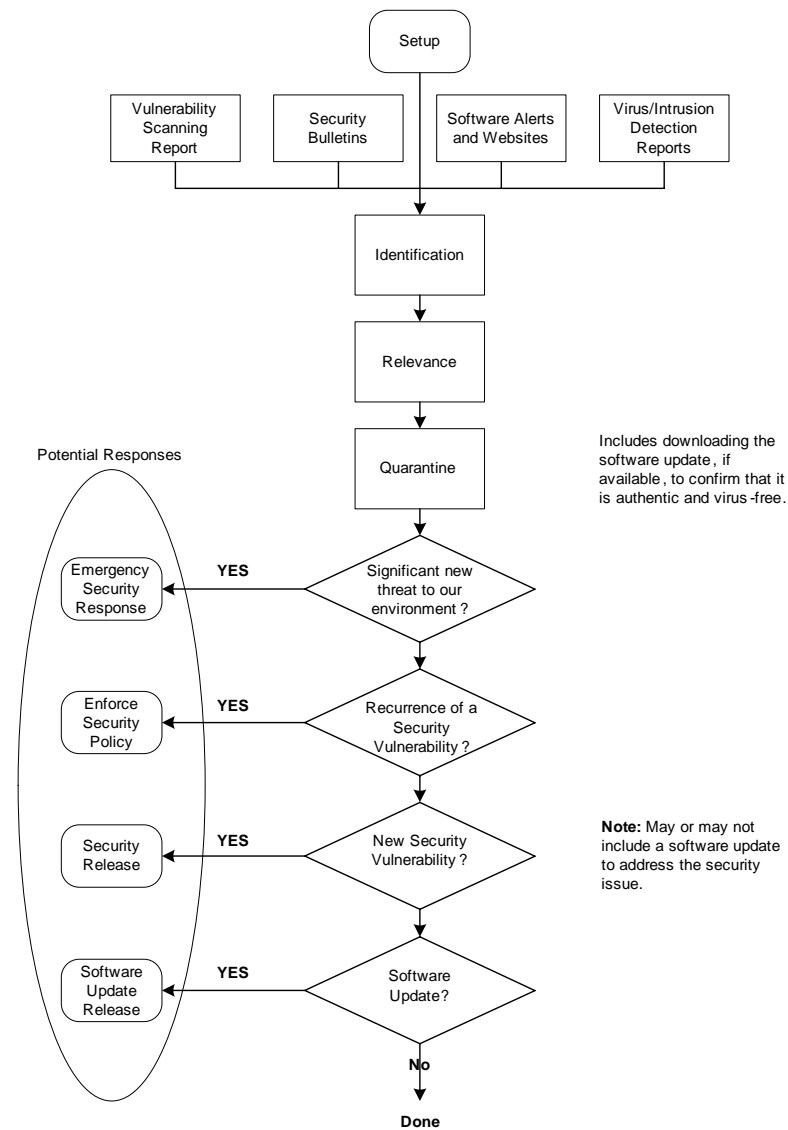


Change Initiation

Change Initiation incorporates all the ongoing activities that determine when action needs to be taken due to a risk or vulnerability. This would include:

1. Tracking vendor's security issues and related software updates
2. Reviewing Security Bulletins
3. Reviewing vulnerability Scanning report
4. Reviewing Software alerts
5. Virus-Intrusion detection reports

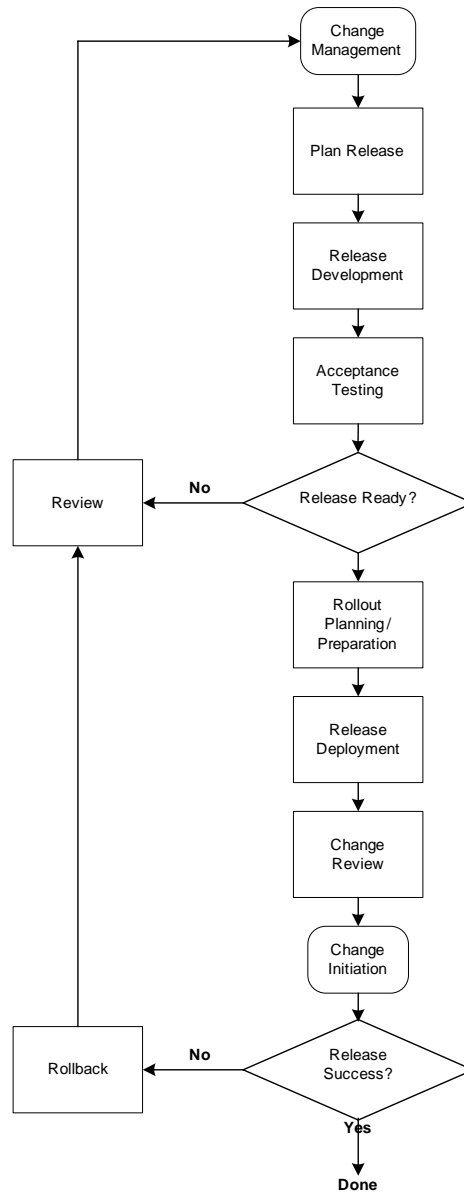
Once an issue is identified then relevance and risk to your system must be determined.



Security Patch Release

The Security Patch Release is predicated on the identification of a security risk and the availability of a resolution. The Security Patch Release process usually includes the following actions:

- Change Management - Determining what kind of change is required in the production environment, deploying a software update, applying countermeasures that mitigate the vulnerability, describing the required change so that others can understand and act on it, prioritizing and scheduling a release to implement the change, ensuring the appropriate people authorize and approve the change and proposed release schedule.
- Release Management – Implements the following steps:
 1. Plan release - Defining and prioritizing all requirements for a security release and creating the release plan that includes a test plan, rollout plan, and rollback plan.
 2. Release development - Selecting the release mechanism and designing, building, and testing the release package.
 3. Acceptance testing - Acceptance testing should focus on how the security release and release package performs in test environment that closely mirrors your production system.
 4. Rollout planning and preparation - Finalizing rollout specifics and preparing the infrastructure for the release. Rollout preparation requires the coordination of resources and may include pre-staging of hardware and software.
 5. Release deployment - Distributing and installing the release across the production system that may or may not be implemented in a phased deployment approach.
- Change Review – Monitoring of the system for unexpected problems, conducting a post deployment review to help improve the Security Patch management process.



Virus and Malware Protection

Virus protection is a critical component of a solid security program. Define where and what virus protection is to be implemented and document the proper configurations for the virus protection software. Doing so adds an additional level of security at each access point of the system. Include mandatory virus definition updates.

Threats exist to Critical Assets simply by connecting to the PCN. Computer viruses and worms can be transmitted by a number of means and if implemented on your machine, will cause it to malfunction. The malfunction may result in loss of data, or in some instances, incorrect operation which could result in injury or death.

The following section provides an overview of security capabilities that are available to or being developed in support of the ICS community. There are several security products that are marketed specifically for ICS, while others are general IT security products that are being used with ICS. Many of the products available offer "single point solutions," where a single security product offers multiple levels of protection. In addition to available products, this section also discusses some research and development work towards new products and technologies.

Encryption

Encryption protects the confidentiality of data by encoding the data to ensure that only the intended recipient can decode it. Encryption is also used as a mechanism in data integrity and authentication operations. Encryption products designed specifically for ICS applications are commercially-available, as well as general encryption products that support basic serial and Ethernet-based communications.

In addition to these products, the ICS SCADA community is working to develop a standard for implementing the encryption of SCADA communications. The [American Gas Association](#) is working to develop a standard, AGA-12, Cryptographic Protection of SCADA Communications, to protect SCADA master-slave communication links from a variety of active and passive cyber attacks by developing a set of standards to secure serial communication links using encryption. The AGA effort is broken into four parts, with each addressing different aspects of SCADA communication protection:

- AGA 12-1 summarizes cyber security policies, the background of the cyber security problem, and a procedure for testing cryptographic protection systems.
- AGA 12-2 is a detailed technical specification for building interoperable cryptographic modules to protect SCADA communications for low-speed legacy SCADA systems and dial-up maintenance ports.
- AGA 12-3 will describe how to protect high-speed SCADA communications over networked systems.
- AGA 12-4 will describe how to build next-generation SCADA systems with embedded AGA 12 compatible cryptography.

Note Because of the long life of SCADA systems, a decision was made to focus initial efforts on the protection of legacy systems.

Firewalls

Firewalls are commonly used to segment networks to protect and isolate ICSs. These implementations use commercially available firewalls that are focused on Internet and corporate application layer protocols and are not equipped to handle ICS protocols. The ICS community is investigating the possibility of adding protocol awareness to filtering devices.

Research was performed by an IT security vendor in 2003 to develop a Modbus-based firewall: a netfilter/iptables extension that allows policy decisions to be made on Modbus/TCP header values just as traditional firewalls filter on TCP/UDP ports and IP addresses [61]. However, to date no commercial product has been released with a Modbus firewall capability.

Intrusion Detection and Prevention

Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs) are being deployed on ICS networks and components to detect well-known cyber attacks.

- Network IDS products monitor network data and compare it to signatures of known attacks and vulnerabilities.
- Host intrusion detection uses software loaded on a host computer with attack and vulnerability signatures to monitor ongoing events and data on a computer system for possible exploits.

IPS products take intrusion detection a step further by automatically acting on a detected exploit.

The ICS security team must constantly monitor, evaluate, and quickly respond to intrusion detection events. This function is sometimes contracted to a managed security service provider (MSSP). MSSPs have correlation and analysis engines to process and reduce the vast amounts of events logged per day to a small subset that needs to be manually evaluated.

Correlation and analysis engine products are available to large organizations wanting to perform this function in-house. Security event management (SEM) products are used in some organizations to monitor, analyze, and correlate events from IDS and IPS logs, as well as audit logs from other computer systems, applications, infrastructure equipment and other hardware and software, to look for intrusion attempts.

IDS and IPS Developments

Current IDS and IPS products are effective in detecting and preventing well-known Internet attacks, but until recently they have not addressed ICS protocol attacks. IDS and IPS vendors are beginning to develop and incorporate attack signatures for various ICS protocols such as Modbus, DNP, and ICCP.

- One cooperative effort within the ICS community is developing Snort rules for Modbus TCP, DNP3, and ICCP. Snort is an open-source network intrusion prevention and detection system using a rule-driven language to perform signature, protocol, and anomaly-based inspections.

The current rulesets, covering Modbus, DNP, and ICCP, are basic, and efforts are underway to expand them. The rules are available at no cost to any ICS user, vendor, integrator, or consultant. The documentation, test data, and configuration files are also available at no charge.

- These same vendors are also defining a data dictionary of log entries from various ICS applications. The data dictionary helps cyber security monitoring products and services identify and understand the meaning of security events in ICS application logs using normalized events. The dictionary is still under development.

Note As with any software added to an ICS component, the addition of host IDS or IPS software could affect system performance.

IPSs are commonplace in today's information security industry. These systems have the ability to automatically reconfigure systems if an intrusion attempt is identified. Automated and rapid reaction is designed to prevent successful exploits; however, an automated tool like this could be used by an attacker to adversely effect the operation on an ICS by shutting down segments of a network or server. False positives can also hinder ICS operation.

Malware/Antivirus Software

Early malware threats were primarily viruses, so the software to detect and remove malware has historically been called "antivirus software," even though it can detect many types of malware. Antivirus software is used to counter the threats of malware by evaluating files on a computer's storage devices against an inventory of malware signature files.

If one of the files on a computer matches the profile of known malware, the malware is removed through a disinfection process so it cannot infect other local files or communicate across a network to infect other files on other computers. Techniques are available to identify unknown malware "in-the-wild" when a signature file is not yet available.

Many ICS end-users and vendors recommend the use of COTS antivirus software with their systems, and have even developed installation and configuration guidance based on their own laboratory testing. Some ICS vendors recommend the use of antivirus with their products, but offer little to no guidance. Some end users and vendors are hesitant to use antivirus software due to fears that its use would cause ICS performance problems or even failure.

Note NIST and [Sandia National Laboratories \(SNL\)](#) are conducting a study and producing a report aimed at helping industry to deploy antivirus software and to minimize and assess performance impacts of workstation and server-based antivirus products. This study has assembled a vast amount of ICS-based antivirus knowledge into a single document, which serves as a starting point or a secondary resource when installing, configuring, running, and maintaining antivirus software on an ICS.

In many cases, performance impacts can be reduced through configuration settings as well as antivirus scanning and maintenance scheduling outside of the antivirus software practices recommended for typical IT systems. This cooperative industry effort has also made antivirus software vendors more aware of ICS and their special performance requirements, initiating better communications within the two fields.

In summary, commercial off-the-shelf (COTS) antivirus software can be used successfully on most ICS components. However, special ICS specific considerations must be taken into account during the selection, installation, configuration, operational, and maintenance procedures. ICS end-users should consult with the ICS vendors regarding the use of antivirus software and can also use the output of the NIST and SNL study as supplemental information.

Vulnerability and Penetration Testing Tools

Many tools are available for performing network vulnerability assessments and penetration tests for ICSs; however, the impacts these tools may have on the operation of an ICS must be carefully considered.

The additional traffic and exploits used during active vulnerability and penetration testing, combined with the limited resources of many ICSs, have been known to cause ICSs to malfunction. As guidance in this area, SNL has developed a preferred list of vulnerability and penetration testing techniques for SCADA systems. These are less intrusive methods, passive vs. active, to collect the majority of information that is often queried by automated vulnerability and penetration testing tools. These methods are intended to allow collection of the necessary vulnerability information without the risk of causing a failure while testing.

In addition to tools, there are several security consultants available that offer vulnerability and penetration services. ICS owners must make these consultants aware of the criticality of continuous operation and the risks involved with performing these tests on operational systems. It may be possible to mitigate these risks by performing tests on ICS components such as redundant servers or independent test systems in a laboratory setting.

Summary

Customers should scan their machines and networks for computer viruses and malware. Many companies, including Microsoft, provide solutions for these issues. Customers should work closely with their IT departments to correctly deploy these scanners and use them in conjunction with applications, especially those requiring nearly all dedicated machine resources.

Wonderware Technical Support provides guidance in the use of several virus scanners and tools, and further information is available to help customers make decisions about scanning and detection tool software in their environments.

With the many Host-based protection system options available on the market today, one must ensure that when selecting this protection component that all Supervisory and Control system software is compatible and that the vendor provides timely updates so your protection is continuously current. Host-based protection software should also provide protection for other malicious software such as Spyware, Malware, and Adware.

Technical References

Note that it has been observed when using AntiVirus software, that control system functionality may be stopped while the software performs various functions. Please see Wonderware Tech Article 2098, "AntiVirus and Malware Removal in the FactorySuite A² and ArchestrA Environment: Security Considerations." There is also a white paper available entitled "Using AntiVirus and Malware Removal Tools in PCN and SCADA Environments" which describes the same issues.

C H A P T E R 5

ICS Security Recommendations

The ability to secure an Industrial Control System (ICS) is directly related to the infrastructure or operating system platform.

The recommended approach to securing a system is to implement the system in Secure Areas and Layers using IPSec, commonly referred to as Defense-in-Depth.

Contents

- Security Perspective
- Control System Industry LAN Security Recommendations
- Control System Industry SCADA Security Recommendation
- Defining the Secure Process Control Environment
- The OSI Model and Securing a Control System
- Using IPSec to Secure Control Systems
- Defining the ICS Security Layers

Security Perspective

Information systems in manufacturing facilities are evolving rapidly and along with the technological advances come security risks. The evolution of these information systems is driven by manufacturers' need for easier integration, easy access to data, and lower maintenance costs.

Wonderware provides customers in the manufacturing sector with the flexible, scalable products that they need while also ensuring that those products are resistant to security risks.

Product Security Statement

Wonderware provides high-quality, secure products designed to meet the the complexity of plant environments and the elements of the security system in those environments.

To address the challenge of delivering open, safe and secure solutions to manufacturing facilities, and facilitate the sharing of information, Wonderware partners with Microsoft and industry standards organizations like the ISA, NIST, PCSF, and the OPC Foundation in order to get multiple vendors involved in an industry-wide approach to solving security problems.

The following sections describe IT and Control System Security Perspective

Defining Computer Interactions

Computer interactions within the Corporate Business environment are fundamentally different than computer interactions within a Control System environment. The practical result of the different interactions is that the IT and Industrial Control System Operations groups view security from opposite perspectives.

The following sections describe the node relationships that drive security implementation in the Business/Corporate- and the ICS/SCADA environments.

Business/Corporate Node Interactions

Computers in a corporate networking environment are generally divided into two groups: Clients and Servers. While this model has been stretched lately with the advent of new software and programming philosophies, the intent and purpose of the client machines' role is to connect in a one-to-one fashion (client-to-server), after security conditions have been satisfied.

Additionally, Server computers are configured not to trust any machine connecting to them, and client machines are usually prevented from interacting freely with one another for, if nothing else, privacy reasons, let alone the security and isolation concerns should one become infected.

ICS or SCADA Node Interactions

The security model on the plant floor machines (in the ICS/SCADA environment) is almost diametrically opposite of the Business/Corporate environment.

Within an Industrial Control System or ICS, the entire system of interconnected computers and networked devices and machines is viewed as a single end device. It is then easy to see that devices are connected together in order to create a parallel-computing, steady-state environment. The machines in this environment need to communicate freely with each other, and the data flow between machines is far more important than if each machine within the enterprise were individually secured against every other machine on the network.

This is because of each individual machine's role. In this context, the "role" is described as a specific function within the greater system.

Inter-Dependent Roles

The services running on a computer are highly inter-dependent. If any of them are shut off or stopped, or if communication is disrupted or data flow is interrupted between any of them, the computer will behave unpredictably or stop altogether.

Imagine what would happen if you stopped the Kerberos service on your computer. Kerberos queries, encrypts and delivers security clearance for both User credentials and any Services credentials to all administrative processes requiring them, including everything requiring permissions to start, run, open, view, change, browse, add content to, get content from, save, or even logon to a computer. Stopping that service would simply and effectively stop the computer from operating in any sort of predictable manner.

Each node within the Industrial Control system has a specific role, which never changes by its own accord. Barring any nodes' failure, it will always continually operate in a predictable manner. The system nodes interact with each other openly and freely; i.e. inter-dependently.

Within a ICS/SCADA environment, different system nodes require ongoing data, telemetry, commands and credentials from other nodes on the system. All distributed process control systems operate more or less the same way, and always intentionally and predictably.

IT Practices in the ICS/SCADA System

Imposing artificial changes on the way the production nodes work together (adding an OS security patch, installing third-party software, or closing communication ports) will very likely disrupt the process control system.

Limiting connectivity and functionality between these ICS nodes may cause the system to break somewhere, usually in an unpredictable and uncontrollable manner. The nodes must inherently and implicitly trust one another in order to operate properly.

Third Party Applications in the Control Environment

Another important issue in the consideration of steady-state control system design is that all third-party software is increasingly taking larger portions of each machine's primary purpose resources for their own purposes.

Third Party Change Catalysts

First, it is far easier to write more code for software programs to add new features or make some feature operate differently, than it is to write a newer, more efficient program.

Even so, many times, software authors or QA personnel do not go to the levels of application efficiency testing that is required to exist concurrently on machines with primary purposes other than theirs. Instead, software developers expect machine resources to continually increase as time goes on. Indeed, it is virtually impossible to run much modern software on a machine built 5 years ago.

Another factor involving the use of third party software is that the numbers of viruses and worms (that the antivirus software scans for) increases over time. Third party virus-scanning programs must consume more and more resources over time. Resources are not limited to only machine memory and hard drive usage, but also include processing time. In a time-critical environment such as an Industrial Control System, this is a luxury that is simply not available or practical.

Altering IT Strategies

It is necessary to alter the current thinking and philosophy of current IT Department continual security patch upgrading and use of resource intensive 3rd party scanning software.

In a process control environment where every element running in it is required to be steady-state, applying standard IT security strategies will affect the continued operation of the Industrial Control System in some negative and unpredictable manner. It is simply a statistical probability that a significant event will occur at some time when continuous unpredictable changes to ICS connectivity and feature sets continue on an ongoing basis.

The following recommendations focus on implementing strategic change.

Current Strategy: Apply Ad Hoc Upgrades and Patches

The current reactive security strategy is to simply apply the changes and continually "fix" the ICS as fast as any new "bad stuff" is announced or found out.

The scenario usually plays out in the following manner:

When new "bad stuff" is found, there is a lot of scrambling and mountains of effort: First, by the OS vendor to build security patches; then by the reactionary scrambling and mountains of effort of the primary purpose software vendor; and sometimes, but not always, the concurrent and sometimes duplicate mountains of effort and scrambling by any third party software used concurrently in the PCN.

When that's all done, the end user (you) begins scrambling and extra work if something is discovered to be broken after applying the upgrade or patch:

- Contact the primary purpose software vendor.
- Make the required changes.
- (Possibly) contact the third party solution vendor.

Either vendor may go back to the OS vendor, who writes more patches. The end user installs them and provides feedback again and on and on and on and on and on...

This is exactly the nightmare that the industrial control community is currently living out.

This strategy is fraught with problems and involves huge amounts of downtime on your part just to keep up with the changes.

Defining the Standard IT Security Environment

The second change strategy is a methodical approach and requires re-defining the IT security implementation within the boundaries of the control system.

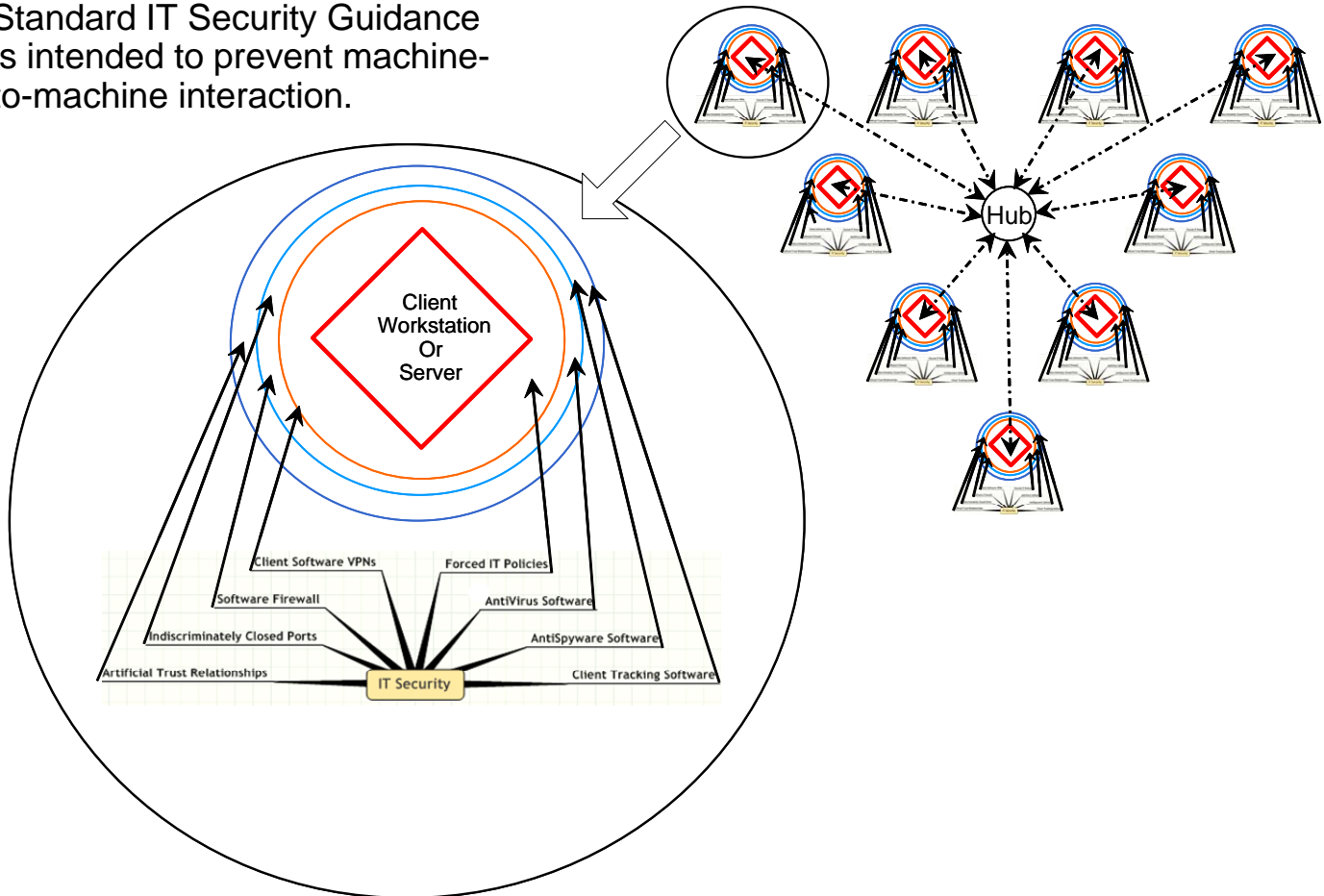
In a normal IT environment, the machines installed are usually divided into two groups called either "Clients" or "Servers." There is a traditional security model that is applied to each of these machines based on their believed functionality and also based on the fact that they implicitly should not trust each other.

Client machines are set up not to trust or communicate to other client machines. Server machines are designed to not trust client machines and also, oddly enough, not to trust other server machines. The theory however is that if any server machines are infected by a client machine, the infection probably would not spread if the trust between servers is made difficult.

The client machines in this environment are often connected to unpredictable and unsecure areas, and are exposed to a variety of infection vectors without any warning, and sometimes are infected without apparent immediate consequence, but may release viral or worm payloads at some predestinated time in the future to the local machine and if possible to any other unsuspecting domain member.

In this kind of environment each machine must be as strong and protected as much as possible, even to the extent of limiting or seriously impairing the functionality of each machine. Establishing communications between machines in this type of environment is extremely difficult and sometimes impossible based upon the rules established by the IT Department in charge of them. The weakest link in the system is the machine most poorly protected and exposed to the highest infection vectors.

Standard IT Security Guidance is intended to prevent machine-to-machine interaction.



Defining the ICS Security Environment

In a control system environment, the individual machines may be either a client or a server or both, and usually exist in a peer-to-peer configuration. Because they have specifically designed and predictable functionality, machines running in that environment rely on a high level of trust and to be highly trusted by the other machines in the enterprise. This environment is sometimes called a Parallel Computing Environment, and may be better known as a peer-to-peer automation system.

These machines all operate in a consistent steady-state type of environment. Unpredictable changes to any machines within an environment operating in this mode may result in unpredictable behavior, and actual ramifications to physical machinery or plant processes that can result in serious situations.

Traditional IT security techniques applied to this environment can have disastrous consequences. Stories of millions of dollars of product or equipment losses have been reported with additional loss of control of the environment and loss of life and/or environmental damage travel throughout the industry quite frequently. A detailed analysis of the problems of applying security to this Parallel Computing Environment using traditional IT methodology shows glaring omissions and unacceptable levels of risk for modern control systems, things which should have been mitigated by design, well before implementation was applied to the system.

Secure ICS Network Requirements

The following information explains several important requirements for standard network topologies implemented as a Process Control Network (PCN) or SCADA system:

The system must maintain a prevention philosophy to support security policies and procedures that include the following attributes:

- Layering Techniques using adjacent-layer disparate technologies
- Firewall Devices and Secure Network Routing
- Secure Network Packaging
- Network-based Intrusion Prevention/Detection
- Clearly defined change management policy (For example: OS Security Upgrades)
- Single-Point Convergence of IT and Plant networks
- No Secured and Unsecured protocols existing on the same domain
- Monitoring, alerting and diagnostics of plant network control systems and their integration to the corporate network
- Support for secure off-platform data and automation clients
- Archiving forensic information to support investigation/legal litigation
- Ensure secure connectivity to wireless devices

All these elements can then be considered as a single endpoint device.

Defining the Single Endpoint Device

The number one criteria to define and understand the Secure Control System Enterprise is to consider, construct, and maintain it as a **single endpoint device**. In Microsoft terminology, this is called domain isolation. See Appendix 5, "ICS Security Recommendations," for guidance in configuring it. Additionally Appendix A contains several useful links to detailed Microsoft guidance for using and configuring domain isolation.

By maintaining this philosophy, understanding, and viewpoint throughout the design, implementation, and maintenance phases, you will identify current and potential system problems, weaknesses, vulnerabilities, and risks. These issues are attributed to unsecure System/Software configuration limitations or User access needs that are poorly-implemented.

Once identified, the issues may be removed and/or mitigated to provide improved security without impact on (or in some cases, with an improvement in) operational performance.

At the same time, the security solution for the ICS is greatly enhanced during the implementation and integration project phases by pooling IT security expertise and the Control System Operations groups. This strategy ensures that the following elements will be considered and incorporated:

- People
- Processes
- Policies
- Products

Plan for a Single Endpoint Device

Planning for a Single Endpoint Device provides the following benefits:

- The solution is easy to implement and maintain.
- It is much more secure.
- The implemented outcome is virtually entirely predictable.

Planning and design must occur before implementing the security solution.

Summary Security Recommendations

- IT and Process Control Groups must change their ideas about what is (and what is not) meant by the word "secure." Both groups must learn and decide *how* to secure the control system, and both groups must understand (at a fundamental and architectural level) what the various processes are doing while interacting within the control system.
- The IT group cannot simply "configure a box" with what they believe is a secure OS and tell the Process Control Groups to install their software on the machine.
- IT and Process Control Groups cannot consider deploying individual machines within a Process Control Network without first thinking about the impact on the entire system.
- It is no longer practical to allow indiscriminate changes to ICS/SCADA system nodes.
- Both groups must understand how the nodes on the ICS/SCADA system connect.
- A Corporate network absolutely must be viewed as "compromised" and there is no safe alternative to these summary recommendations.

Security Recommendations Justification

Every day random parts of a corporate business network travel to dangerous places full of virulent malware code in a myriad of unpredictable manners. Installation of various scanner software, "black boxes," restrictive policy implementation, and tracking tools are used in an attempt to reduce the surface area of exposure to this environment. This type of implementation is called a "reactive" security environment. It is not effective or safe to trust a complete manufacturing or control system enterprise to marketing claims of various "security system" manufacturers, especially ones who do not normally work within the realms of ICS or SCADA System domains.

It only takes ONE bad virus or malware component to penetrate the ICS and stop the entire system. A thorough risk analysis shows that such a single point of failure to be completely intolerable within the ICS/SCADA environment and that the security risk must be mitigated. Unintentionally stopping an ICS can cost millions of dollars: in unmade or ruined product with unused raw materials needing to be discarded in some cases. Also, possible cascade failure of plant processes, perhaps resulting in environmental damage or even loss of life are possibilities of this scenario.

Business justification for security upgrades is often difficult to create until an actual breach occurs, then swift and usually not-well-thought out Draconian-style policies are usually imposed on the domain and individual machines. This is a completely reactive response to security and it has proven historically to never be very effective for any length of time, and also tends to break the peer-to-peer, parallel computing ICS environments.

Instead, it is important to grasp security concepts and apply them systemically to your individual environment. Therefore, there is a requirement to stay up to date in understanding the changing threats to your systems, and continually utilize methodology to minimize those threats, instead of waiting for someone else to provide a fix for you. This is the basis of proactive security.

Attempts have been made to quantify and justify ROI calculation methodology for security, the same way it is done with safety upgrades. Unfortunately application of security does not provide any immediate measurable output which can be compared against money spent, except a subjective feeling that the system is "probably" more secure than it was before the expenditures. When calculating Safety ROI, benefit for money spent is usually directly observable and measurable, but not so with Security.

There are no empirical measurements to state that any given system is such-and-such amount more secure than it was before spending a given amount of money on security appliances or techniques. Instead, security must be systemic and understood at a fundamental level. It must be measured using statistical tools including probability of attack by specific vectors, risk analyses, and mitigation strategies until it is felt and observed that the leftover unmitigated risks can be tolerated by the company. At this writing, some research is being done with ROI calculations being based on "mean time to failure." This value is still experimental, but may assist in creating security ROI calculations in the future.

This Security Guidance Manual is only a beginning, a "Guide" of best practices designed to assist in determining what is and is not safe within your enterprise. There are no "cookie cutter" answers for this problem, unless your Industrial Control System is "exactly" like another one, which is very unlikely. Even ICS or SCADA Systems designed to be "identical" contain differences and variants, and each variant can introduce a potential threat vector into the system.

You must plan for and mitigate security risks ahead of time. When the Process Control or SCADA System is complete and running properly, the greatest asset you have against threat vectors is the system itself. Unlike the current IT solutions on a Corporate Network, your PCN will tell you immediately when something is wrong. It is, by design and definition, a single machine that operates in a specific and predictable manner. If it does not operate as designed, it needs to be stopped and fixed before the process goes out of control and makes bad product or worse. This is the essence of Statistical Process Control, and is also the basis of keeping your system secure and operating efficiently for many years.

Control System Industry LAN Security Recommendations

The best practice recommendation for an ICS is to completely separate the process control network from the enterprise network. The nature of network traffic on these two networks is different:

- Internet access, FTP, email, and remote access will typically be permitted on the enterprise network but not on the process control network.
- Rigorous change control procedures for network equipment, configuration, and software changes may not be in place on the enterprise network.
- If process control network traffic is carried on the enterprise network, it could be intercepted. By having separate networks, security and performance problems on the enterprise network should not be able to affect the process control network.

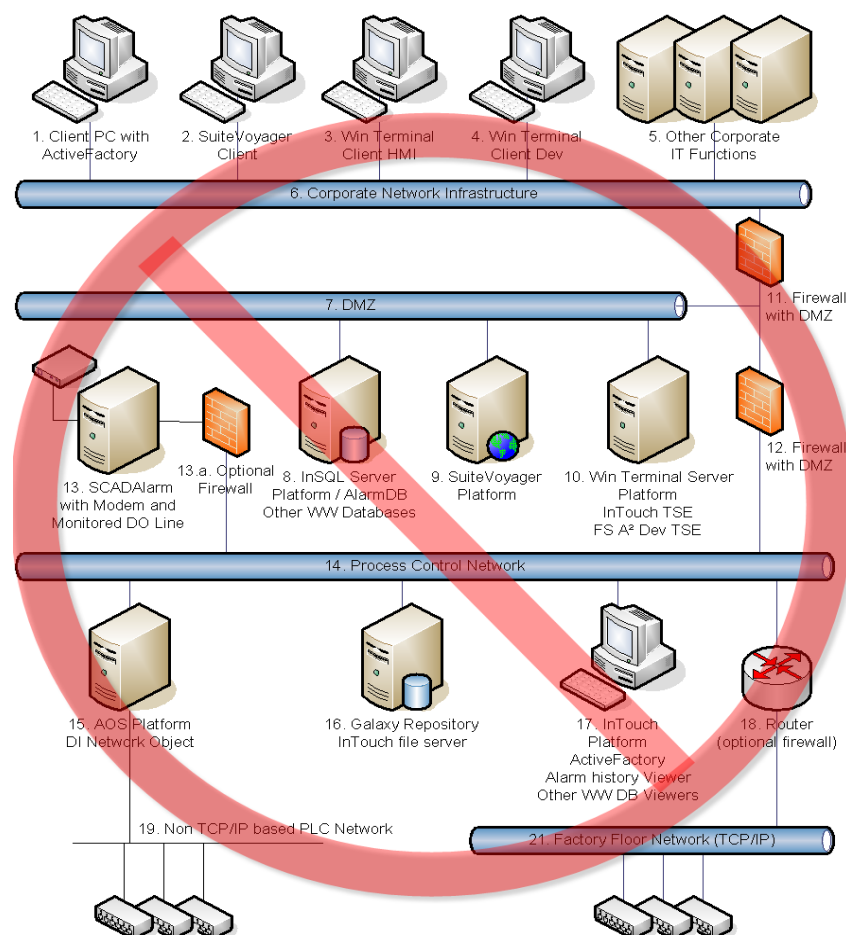
However, practical considerations often mean that a connection is required between the process control and enterprise networks. This connection is a significant security risk and careful consideration should be given to its design.

If the networks must be connected, it is strongly recommended that only a single connection be allowed, and that the connection be through a firewall, or better yet an Active Intrusion Prevention System (IPS) appliance. Also, establish a demilitarized zone (DMZ) for any data warehouse or data warehouse proxy (recommended for a very secure configuration).

A DMZ is a separate network segment that connects directly to the firewall. Servers containing data from the process control system, which need to be accessed from the enterprise network, are put on this network segment. Only these systems should be accessible from the enterprise network. With any external connections, the minimum access should be permitted through the firewall. Only the ports required for specific communication should be opened to the external environment.

The following sections describe the access required for specific node types.

The following graphic describes most Control Systems industry security guidance based on the "business domain" model:



This configuration is no longer recommended.

Implementing Network Firewalls

Network firewalls are devices or systems that control the flow of network traffic between networks employing differing security postures. In most modern applications, firewalls and firewall environments are discussed in the context of Internet connectivity and the TCP/IP protocol suite.

Firewalls have applicability in network environments that do not include or require Internet connectivity. For example, many corporate enterprise networks employ firewalls to restrict connectivity to and from internal networks servicing more sensitive functions, such as the accounting or personnel department. By employing firewalls to control connectivity to these areas, an organization can prevent unauthorized access to the respective systems and resources within the more sensitive areas.

Firewall Types

The following section describes three general classes of firewalls:

- **Packet Filtering Firewalls:** The most basic type of firewall is called a packet filter. Packet filter firewalls are essentially routing devices that include access control functionality for system addresses and communication sessions. The access control is governed by a set of directives collectively referred to as a ruleset.

In their most basic form, packet filters operate at layer 3 (network) of the Open Systems Interconnection (OSI) model. This type of firewall checks the address information in each packet of data to a set of criteria before forwarding the packet. Depending on the packet and the criteria, the firewall can drop the packet, forward it, or send a message to the originator.

Note For information on the OSI model, see "The OSI Model and Securing a Control System" on page 185.

The advantages of packet filtering firewalls include low cost and low impact on network performance, usually because only the source address in the packet is examined. For example, the IP source address of each packet is identified, then an established rule determines if the packet should be discarded or forwarded.

- **Stateful Inspection Firewalls:** Stateful inspection firewalls are packet filters that incorporate added awareness of the OSI model data at layer 4. Stateful inspection firewalls filter packets at the network layer, determine whether session packets are legitimate, and evaluate the contents of packets at the application layer.

Stateful inspection keeps track of active sessions and uses that information to determine if packets should be forwarded or blocked. It offers a high level of security and good performance, but it is expensive. Due to its complex nature, it can be less secure than simpler types of firewalls if not administered by highly competent personnel.

- **Application-Proxy Gateway Firewalls:** This firewall type examines packets at the application layer and filters traffic based on specific application rules, such as specified applications (e.g., browsers) or protocols (e.g., File Transfer Protocol [FTP]). It offers a high level of security, but has a significant impact on network performance.

[NIST SP 800-41, Guidelines on Firewalls and Firewall Policy](#), provides general guidance for the selection of firewalls and the firewall policies.

Deploying Firewalls in the ICS

In an ICS environment, firewalls are most often deployed between the ICS domain and the corporate LAN. Properly configured, they can greatly restrict undesired access to and from control system host computers and controllers, thereby improving security. They can also potentially improve a control network's responsiveness by removing non-essential traffic from the network.

When designed, configured, and maintained properly, dedicated hardware firewalls can contribute significantly to increasing the security of today's ICS environments.

Firewall Functionality

Firewalls provide several tools to enforce a security policy that cannot be accomplished locally on the current set of process control devices available in the market, including the ability to:

- Block all communications with the exception of specifically enabled communications between devices on the unprotected LAN and protected ICS networks. Blocking is based on source and destination IP address pairs, services, and ports. Blocking can occur on both inbound and outbound packets to limit high-risk communications such as e-mail.
- Enforce secure authentication of all users seeking to gain access to the ICS network. There is flexibility to employ varying protection levels of authentication methods including simple passwords, complex passwords, two-factor authentication technologies, tokens, and smart cards. Select the particular method based upon the vulnerability of the ICS network to be protected, rather than using the method that is available at the device level.
- Enforce destination authorization. Users can be restricted and allowed to reach only nodes on the control network necessary for their job function. This reduces the potential of users intentionally or accidentally gaining access and control of devices for which they are not authorized, but adds to the complexity for on-the-job-training or cross-training employees.
- Record information flow for traffic monitoring, analysis, and intrusion detection.

Other possible deployments include using either host-based firewalls or small standalone firewalls in front of, or running on, individual control devices. Using firewalls on an individual device basis can create significant management overhead, especially in change management of firewall configurations.

Several issues must be addressed when deploying firewalls in industrial control systems environments, with particular emphasis on the following:

- The possible addition of latency to control system communications.
- The lack of experience in the design of filter rule sets suitable for industrial applications. Firewalls used to protect control systems should be configured so they do not permit either incoming or outgoing traffic by default. The default configuration should only be modified when it is necessary to permit connections to or from trusted systems.

Although industrial control system networks do not often change, hardware firewalls do require ongoing support, maintenance, and backup. Rulesets must be reviewed to ensure they provide adequate protection in light of ever-changing security threats. System capabilities, such as available disk space, must be monitored to make sure that the firewall is performing its data collection tasks and can be depended upon in the event of a security violation.

Using Firewalls to Separate the Control Network

The process control network should be logically separated from the enterprise network on physically separate network devices. When enterprise connectivity is required:

- There should be a single access point between the process control network and the enterprise network.
- A stateful firewall between the process control network and enterprise network should be configured to deny all traffic except that which is explicitly authorized.
- The firewall rules should at a minimum provide source and destination filtering (by IP or media access control [MAC] address), in addition to Transmission Control Protocol (TCP) and User Datagram (UDP) Protocol port filtering and Internet Control Message Protocol (ICMP) type and code filtering.

DMZ Network

Implementing an intermediate DMZ network is an acceptable approach to enabling communication between a process control network and a business domain or network. The DMZ should be connected to the firewall so that specific (restricted) communication may occur between only the enterprise network and the DMZ, and the process control network and the DMZ; the enterprise network and the process network should not communicate directly with each other. Data warehouse proxies are usually placed in this environment.

Segmenting the Process Control and Enterprise Networks

Process control networks and enterprise networks can be segmented using several different implementation strategies. The following section describes common segmented topology variations and scenarios, and explains the advantages and disadvantages of each.

Dual-Homed Computer

Dual-homed computers can pass network traffic from one network to another. Without proper security controls in place on the computer, network traffic could be placed on a network that poses additional threats. To prevent this, no network component other than firewalls should be configured as dual-homed so that they span both the process control and enterprise networks. All connections between the process control network and the enterprise network should be through a firewall or an active perimeter Intrusion Prevention (IPS) System.

Firewall Between Enterprise Network and Control Network

By introducing a simple two-port firewall between the enterprise and control networks, a significant security improvement can be achieved. Most firewalls on the market offer stateful inspection for all TCP packets and application proxy services for common application layer protocols such as FTP, Hypertext Transfer Protocol (HTTP), and Simple Mail Transfer Protocol (SMTP). Diligently configured, the chance of a successful external attack on the control network is significantly reduced.

Unfortunately, two issues still remain with this design. First, if the Historian resides on the enterprise network, a rule must exist within the firewall allowing the data historian to communicate with the control devices on the control network. A packet originating from a malicious or incorrectly configured host on the enterprise network (appearing to be the data historian) would be forwarded to individual PLCs.

If the data historian resides on the process control network, a firewall rule must exist that allows all hosts from the enterprise to communicate with the historian. Typically, this communication occurs at the application layer as Structured Query Language (SQL) or HTTP requests. Flaws in the historian's application layer code could result in a compromised historian. Once the historian is compromised, the remaining nodes on the process control network are vulnerable to a worm propagating or an interactive attack. Therefore it is recommended that needed process data be stored in a separate machine called a data warehouse, independently updated from the historian. This data warehouse acts as a proxy for the historian.

Second, spoofed packets can be constructed that can affect the control network, and covert data may be able to be tunneled in allowed protocols. For example, if HTTP packets are allowed through the firewall, then Trojan horse software accidentally introduced on an HMI or control network laptop could be both controlled by a remote entity and send data (such as captured passwords) to that entity, disguised as legitimate traffic.

In summary, while this implementation is a significant improvement over a non-segmented network, it requires the use of firewall rules that allow direct communications between enterprise and ICS devices. This can result in possible security breaches if not very carefully designed and monitored.

Firewall and Router between Enterprise Network and Control Network

A slightly more sophisticated topology design is the use of a router/firewall in combination. The router sits in front of the firewall and offers basic packet filtering services, while the firewall handles the more complex issues using either stateful inspection or proxy techniques. This type of design is very popular in Internet-facing firewalls because it allows the faster router to handle the bulk of the incoming packets, especially in the case of denial of service (DoS) attacks, and reduces the load on the firewall. It also offers improved defense in depth since the attacker must bypass two very different devices.

Firewall with DMZ between Enterprise Network and Control Network

Using firewalls with the ability to establish a DMZ between the enterprise and process control networks is a significant security improvement. Each DMZ holds a separate "critical" component, such as the data historian, the wireless access point, or remote and third party access systems. In effect, the use of a DMZ-capable firewall allows the creation of an intermediate network.

Creating a DMZ requires that the firewall offer three or more interfaces, rather than the typical public and private interfaces. One of the interfaces is connected to the enterprise, the second to the ICS network, and the remaining interfaces to the shared or insecure devices such as the data historian server or wireless access points.

By placing enterprise-accessible items in the DMZ, no direct communication paths are required from the enterprise network to the ICS; each network effectively ends in the DMZ. Most sophisticated firewalls can allow for multiple DMZs, and can specify what type of traffic may be forwarded between zones.

The firewall can block arbitrary packets from the enterprise network from entering the control network, and can also regulate traffic from the other network zones. By judicious use of access control lists, a clear separation can be maintained between the control network and other networks, with little or no traffic passing directly between the enterprise and control networks.

Patch and Antivirus Management Server

If a patch management server or an antivirus server is to be used for the control network, it should be located directly on the DMZ. Both functions could reside on a single server. Having patch management and antivirus management dedicated to the control network allows for controlled and secure updates that can be tailored for the unique needs of the process control environment. It is also helpful if the antivirus product that is supported by the process control vendor is not the same as the antivirus product supported by the corporate IT department.

The primary security risk in this topology type is that if a computer in the DMZ is compromised, it can be used to launch an attack against the control network via application traffic permitted from the DMZ to the control network. This risk can be greatly reduced if a concerted effort is made to harden and actively patch the servers in the DMZ and if the firewall ruleset permits only connections between the control network and DMZ that are initiated by control network devices.

Other concerns with this architecture are the added complexity and the increased cost of firewalls with three or more ports. For more critical systems, however, the improved security should more than offset these disadvantages.

Paired Firewalls Between the Enterprise Network and the Control Network

A variation on the firewall with DMZ solution is to use a pair of firewalls positioned between the enterprise and process control networks.

Common servers such as the data historian are situated between the firewalls in a DMZ-like network zone sometimes referred to as a Manufacturing Execution System (MES) layer. The first firewall blocks arbitrary packets from proceeding to the process control network or the shared historians. The second firewall can prevent unwanted traffic from a compromised server from entering the control network, and prevent control network traffic from impacting the shared servers.

If firewalls from two different manufacturers are used, then this solution may offer an advantage. It also allows the process control group and the IT group to have clearly-separated device responsibility since each can manage a firewall on its own. The primary disadvantage with two-firewall architectures is the increased cost and management complexity.

For environments with stringent security requirements or the need for clear management separation, this implementation has some strong advantages.

Network Segmentation Summary

Non-firewall based solutions will generally not provide suitable isolation between control networks and enterprise networks. The two-zone solutions are marginally acceptable but should be only be deployed with extreme care.

The most secure, manageable, and scalable control network and enterprise network segregation architectures should be based on a three-zone system, or more commonly referred to as a "DMZ".

Summary Firewall Policies for ICSs

Once the firewall architecture is in place, the work of determining exactly what traffic you want to allow through the firewall begins. Configuring the firewall to deny all except for pin-holes absolutely required for business needs is every company's basic premise, but the reality is much more difficult. Exactly what does "absolutely required for business" mean and what are the security impacts of allowing those "pin-holes" through?

For example, many companies considered allowing SQL traffic through the firewall as required for business for many data historian servers. Unfortunately SQL was also the vector for the Slammer worm. The fact is, many important protocols used in the industrial world, such as HTTP, FTP, OPC/DCOM, EtherNet/IP and MODBUS/TCP, are significant security risks.

The following material summarizes some of the key points from the [NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks](#) document.

Rule Design Notes

If one is installing a single two-port firewall without a DMZ for shared servers, particular care needs to be taken with the rule design. At a minimum, all rules should be stateful rules that are both IP address and port (application) specific. The address portion of the rules should restrict incoming traffic to a very small set of shared devices (e.g. the data historian) on the control network from a controlled set of address on the enterprise network. Allowing any IP addresses on the enterprise network to access the server inside the control network is not recommended.

In addition, the allowed ports should be carefully restricted to relatively secure protocols such as HTTPS. Allowing HTTP, FTP or any unencrypted SCADA protocol to cross the firewall is a security risk due to the potential for traffic sniffing and modification.

DMZ Notes

If the DMZ architecture is being used, it is possible to configure the system so that no traffic will go directly between enterprise and control network. With a few special exceptions (noted below) all traffic from either side can terminate at the servers in the DMZ. This allows more flexibility in the protocols allowed through the firewall. For example, MODBUS/TCP might be used to communicate from the PLCs to the Data Historian, while HTTP might be used for communication between the historian and enterprise clients.

Both protocols are inherently insecure, yet in this case they can be used safely as neither actually crosses between enterprise and control network. An extension to this concept is the idea of using "disjoint" protocols in all control network-enterprise communications. That is, if a protocol is allowed between the control network and DMZ then it is explicitly NOT allowed between DMZ and enterprise networks. This design greatly reduces the chance of a worm such as Slammer actually making its way into the control network since the worm would have to deploy two different exploits over two different protocols.

Managing Outbound Traffic

One area of considerable variation in practice is the control of outbound traffic from the control network, which could represent a significant risk if unmanaged. One example, is trojan software that uses HTTP tunnelling to exploit poorly defined outbound rules. Thus it is important that outbound rules be as stringent as inbound rules.

[Appendix A of ISA's SP-99 Technical Report #2](#) contains some example guidelines that help clarify this. A summary of these guidelines follows:

- Outbound traffic through the control network firewall should be limited to essential communications only.
- All outbound traffic from the control network to the enterprise network will be source and destination restricted by service and port using static firewall rules.
- Mapped drives across the control network firewall should be avoided.

In addition to these rules, the firewall should be configured with outbound filtering to stop forged IP packets from leaving the control network or the DMZ. In practice this is achieved by checking the source IP addresses of outgoing packets against the firewall's respective network interface address. The intent is to prevent the control network from being the source of spoofed (i.e. forged) communications, which are often used in DoS Attacks. Thus the firewalls should be configured to forward IP packets only if those packets have a correct source IP address for the control network or DMZ networks.

Finally, Internet access by devices on the PCN should be strongly discouraged.

In summary, the following should be considered as recommended practice for general firewall rule sets:

- The base rule set should be DENY ALL, PERMIT NONE.
- Ports and services between the control network environment and an external network should be enabled and permissions granted on a specific case-by-case basis. There should be a documented business justification with risk analysis and a responsible person for each permitted incoming or outgoing data flow.
- All "permit" rules should be both IP address and TCP/UDP port specific, and stateful if appropriate.
- All rules shall restrict traffic to specific IP address or range of addresses.
- All traffic on the control network is typically based only on routable IP protocols, either TCP/IP or UDP/IP. Thus any non-IP protocol should be dropped.
- Prevent traffic from transiting directly from the control network to the enterprise network. All traffic should terminate in the DMZ.
- Any protocol allowed between the control network and DMZ is explicitly NOT allowed between DMZ and enterprise networks (and vice-versa).
- All outbound traffic from the control network to the enterprise network should be source and destination restricted by service and port using static firewall rules.
- Allow outbound packets from the control network or DMZ only if those packets have a correct source IP address assigned to the control network or DMZ devices.
- Control network devices should not be allowed to access the Internet.
- Control networks shall not be directly connected to the Internet, even if protected via a firewall.
- All firewall management traffic be either via a separate, secured management network (e.g. out of band) or over an encrypted network with two-factor authentication. Traffic should also be restricted by IP address to specific management stations.

The reader is cautioned that these should only be considered as guidelines. A careful assessment of each control environment is required before implementing any firewall rule sets.

Recommended Firewall Rules for Specific Services

Beside the general rules described above, it is difficult to outline all-purpose rules for specific protocols. The needs and best practices vary significantly between industries for any given protocol and should be analyzed on a company-by-company basis.

The Industrial Automation Open Networking Association (IAONA) offers a [template for conducting such an analysis](#), assessing each of the protocols commonly found in industrial environments in terms of function, security risk, worst case impact and suggested measures.

The following section summarizes some of the key points from the IAONA document, and suggested practices from the ISA TR2 Appendix A.

The reader is advised to consult these documents directly when developing rule sets.

Domain Name Service (DNS)

Domain Name Service (DNS) is primarily used to translate between domain names (such as control.com) and IP addresses (such as 192.168.1.1). Most Internet services rely heavily on DNS, but its use on the plant floor is relatively rare at this time. In most cases there is little reason to allow DNS requests out of the control network to the enterprise network and no reason to allow DNS requests into the control network. DNS requests from the control network to DMZ should be addressed on a case-by-case basis. Local DNS or the use of host files is recommended.

Hyper Text Transfer Protocol (HTTP)

Hyper Text Transfer Protocol (HTTP) is the protocol underlying web browsing services on the Internet. Like DNS, it is critical to most Internet services. It is seeing increasing use on the plant floor as an all purpose query tool.

Unfortunately it has little inherent security and has the ability to be a transport mechanism for a very large number of manual attacks and worms. In addition HTTP applications are renowned for having vulnerabilities that can be exploited.

In general, HTTP should not be allowed to cross from the enterprise to the control network. If it is, then HTTP proxies should be configured on the firewall to block all inbound scripts and Java applications. Incoming HTTP connections should not be allowed into the control network as they pose significant security risks. If HTTP services into the control network are absolutely required, it is recommended that HTTPS be used instead and only to very specific devices.

File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP)

The File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) are used for transferring files between devices. They are implemented on almost every platform including many DCS, PLCs and RTUs, since they are extremely well known and use minimum processing power.

Neither protocol was created with security in mind; in the case of FTP the login password is not encrypted and, in the case of TFTP, no login is required at all. Furthermore, some FTP implementations have a history of buffer overflow vulnerabilities. As a result all TFTP should be blocked while FTP should be allowed on outbound sessions only or if secured with additional token-based two-factor authentication and an encrypted tunnel.

Telnet

The Telnet protocol defines an interactive, text-based communications session between a client and a host. It is mainly used for remote login and simple control services to systems with limited resources or to systems with limited security needs.

Telnet is a severe security risk because all telnet traffic, including passwords, is unencrypted and it can allow a remote individual considerable control over a device. Thus inbound Telnet session commands from the enterprise to the control network should be prohibited unless secured with token-based two-factor authentication and an encrypted tunnel. Outbound telnet sessions should be allowed only over encrypted tunnels to specific devices.

Simple Mail Transfer Protocol (SMTP)

The Simple Mail Transfer Protocol (SMTP) is the primary email transfer protocol on the Internet. Email messages are notorious for containing viruses so inbound e-mail should not be allowed to any control network device. Outbound SMTP mail messages from the control network to the enterprise are acceptable and could be used to send alert messages.

Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol is used to provide network management services between a central management console and network devices such as routers, printers and PLCs.

While SNMP is an extremely useful service for maintaining a network, its security weaknesses are infamous. Version 1 and 2 of SNMP uses unencrypted passwords to both read and configure devices (including devices such as PLCs) and in many cases the passwords are well known and cannot be changed. Version 3 is considerably more secure but is still limited in use. Thus SNMP commands both to and from the control network should be prohibited unless it is over a separate, secured management network.

Distributed Component Object Model (DCOM)

The Distributed Component Object Model (DCOM) is the underlying protocol for both the popular OLE for Process Control (OPC) and ProfiNet. It utilizes Microsoft's Remote Procedure Call (RPC) service which has known vulnerabilities that were the basis for the Blaster Worm exploits.

OPC (DCOM) dynamically opens a wide range of ephemeral ports (#1024-#65535) that can be extremely difficult to filter at the firewall.

This protocol should only be allowed between control network and DMZ networks and explicitly blocked between the DMZ and enterprise network. Also, users are advised to restrict the port ranges used by making registry modifications on devices using DCOM.

SCADA and Industrial Protocols

SCADA and industrial protocols, such as MODBUS/TCP, EtherNet/IP and DNP3, are critical for communications to most control devices. These protocols were designed without security in mind and do not typically require any authentication to remotely execute commands on a control device. Thus these protocols should only be allowed within the control network and not allowed to cross into the enterprise network.

Network Address Translation (NAT)

NAT is a service where IP addresses used on one side of the firewall can be mapped to a different set on the other side on an as-needed basis. It was originally designed for IP address reduction purposes so that a company with a large number of devices that occasionally needed Internet access could get by with a smaller set of assigned Internet addresses.

To do this, NAT relies on the premise that not every internal device is actively communicating with external hosts at a given moment. The firewall is configured to have a limited number of outwardly visible IP addresses. When an internal host seeks to communicate to an external host, the firewall remaps the internal IP address and port to one of the currently unused, more limited, public IP addresses -- effectively concentrating outgoing traffic into fewer IP addresses. The firewall must track the state of each connection, and how each private internal IP address and source port was remapped onto an outwardly visible IP address/port pair. When returning traffic reaches the firewall, the mapping is reversed and the packets forwarded to the proper internal host.

For example, a control network device may need to establish a connection with an external, non-control network host (for instance, to send a critical alert email). NAT allows the internal IP address of the initiating control network host to be replaced by the firewall; subsequent return traffic packets are remapped back to the internal IP address and sent to the appropriate control network device.

More specifically, if the control network is assigned the private subnet 192.168.1.xxx and the Internet network expects the device to use the corporate assigned addresses in the range 142.232.yyy.zzz, then a NAT firewall will substitute (and track) a 142.232.yyy.zzz source address into every outbound IP packet generated by a control network device.

Producer-consumer protocols, such as EtherNet/IP and Foundation Fieldbus HSE, are particularly troublesome as NAT does not support the multicast-based traffic that these protocols need to offer their full services.

In general, while NAT offers some distinct advantages, its impact on the actual industrial protocols and configuration should be assessed carefully before it is deployed. Furthermore, certain protocols are specifically broken by NAT because of the lack of direct addressing. For example, OPC requires special 3rd party tunnel software to work with NAT.

Specific ICS Firewall Issues

The following section outlines Firewall issues specific to the Industrial Control System:

Data Historians

The existence of shared control network/enterprise network servers such as data historians and asset management servers can have a significant impact on firewall design and configuration. In three-zone systems the placement of these servers in a DMZ is relatively straightforward, but in two-zone designs the issues become complex.

Placing the historian on the enterprise side of the firewall means that a number of insecure protocols, such as MODBUS/TCP or DCOM, must be allowed through the firewall and that every control device reporting to the historian is exposed to the enterprise side of the network.

On the other hand, putting the historian on the PCN side means other equally questionable protocols, such as HTTP or SQL, must be allowed through the firewall and there is now a server accessible to nearly everyone in the corporation sitting on the control network.

In general, the best solution is to avoid two-zone systems and use a three-zone design, placing the data collector in the control network and the historian component in the DMZ. Even this can prove problematic in some situations. Heavy access from the large numbers of users on the enterprise network to a historian in the DMZ may tax the firewall's throughput capabilities.

One suggested solution is to install two servers; one on the control network to collect data from the control devices and a second on the enterprise network mirroring the first server and supporting client queries. Of course this requires a special hole to be put through the firewall to allow direct server-to-server communications, but if done correctly, this poses only minor risk.

Remote Support Access

Another issue for ICS firewall implementation is the use of 3rd party or remote access into the control network. Obviously any users accessing the control network from remote networks should be required to authenticate using an appropriately strong mechanism such as token-based authentication.

While it is possible for the controls group to set up their own remote access system with two-factor authentication on the DMZ, in most companies it is typically more efficient to use existing systems set up by the IT department. In this case a connection through the firewall from the IT remote access server is needed.

It is suggested that remote support personnel connecting over the Internet or via dialup modems should run the corporate VPN connection client and authenticate using the token based two-factor authentication scheme in order to connect to the general corporate network.

Once connected, they should be required to authenticate a second time at the control network firewall (using two-factor authentication) to gain access to the control network. For companies that don't allow any control traffic traversing the enterprise network in the clear, this will require a cascading or secondary tunnelling solution to gain access to the control network, such as an SSL VPN inside an IPsec VPN.

Multicast Traffic

Most industrial producer-consumer (or publisher-subscriber) protocols operating over Ethernet, such as EtherNet/IP and Foundation Fieldbus HSE, are IP multicast-based.

The first advantage of IP multicasting is network efficiency; by not repeating the data transmission to the multiple destinations, a significant reduction in network load can occur.

The second advantage is that the sending host need not be concerned with knowing every IP address of every destination host listening for the broadcast information.

The third, and perhaps most important for industrial control purposes, is a single multicast message offers far better capabilities for time synchronization between multiple control devices than multiple unicast messages.

Multicasting in IP environments typically occurs through the use of multicast group ID's which are mapped directly onto the class D IP address range (from 224.0.0.0 to 239.255.255.255). Each address is considered a separate "transmission frequency"; a host listening to multicast packets must "tune in" to the group ID (IP address) of the transmission it wishes to receive.

If the source and destinations of a multicast packet are connected with no intervening routers or firewalls between them, the multicast transmission is relatively seamless. However, if the source and destinations are not on the same LAN, forwarding the multicast messages to a destination becomes more complicated.

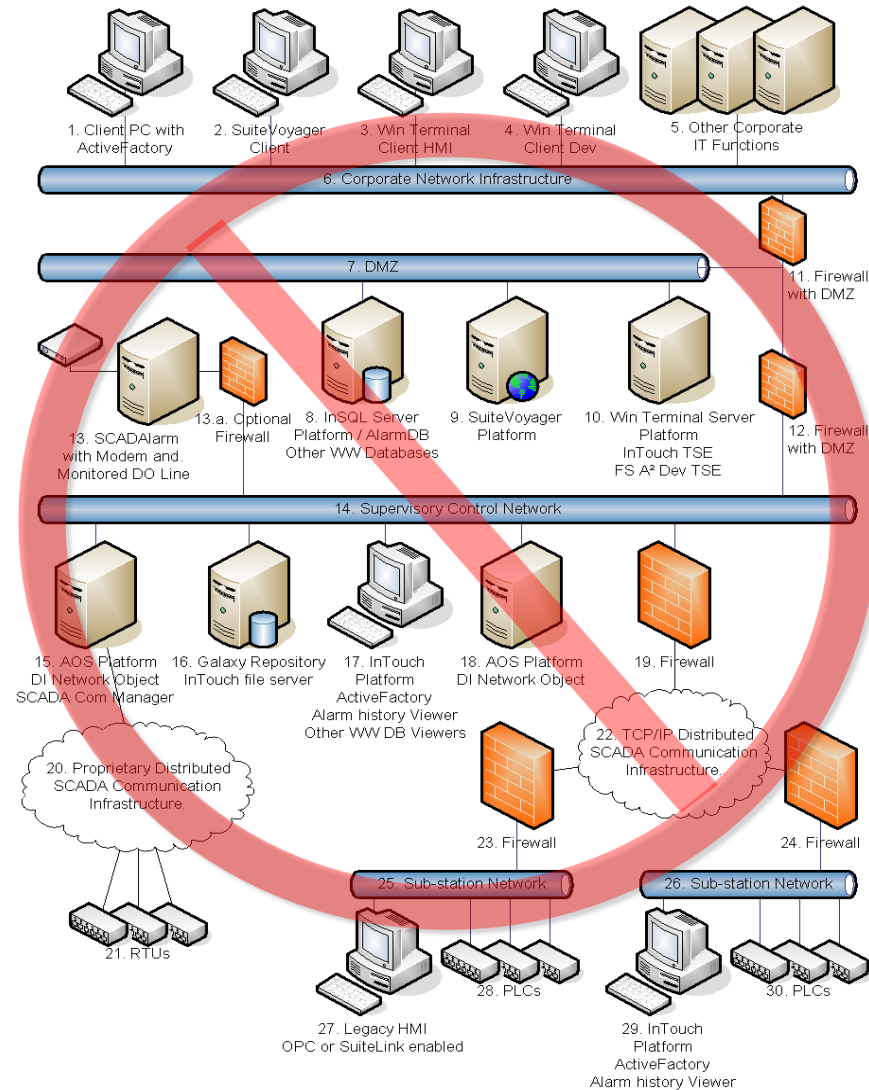
To solve the problem of multicast message routing, hosts need to join (or leave) a group by informing the multicast router on their network of the relevant group ID through the use of the Internet Group Management Protocol (IGMP). Multicast routers subsequently know of the members of multicast groups on their network and can decide whether or not to forward a received multicast message onto their network. A multicast routing protocol is also required.

From a firewall administration perspective, monitoring and filtering IGMP traffic becomes another series of rulesets to manage, adding to the complexity of the firewall strategy.

Another firewall issue related to multicasting is the use of NAT. A NAT'ing firewall receiving a multicast packet from an external host has no reverse mapping for which internal group ID to send the data to. It could, if IGMP-aware, broadcast it to every group ID it knows about (one of them will be correct!), but this could cause serious issues if an unintended control packet was broadcast to a critical node. The safest action for the firewall to take is to drop the packet. Thus multicasting is generally considered NAT-unfriendly.

Control System Industry SCADA Security Recommendation

Customers should be aware that threats exist to Critical Assets simply by connection to the PCN (Process Control Network):



A careful analysis of this fragmented topology shows several serious threat vectors. Many Control System and SCADA implementations using this guidance have led to security breaches, failures, successful attacks, takeovers, and infections through the inter connectivity points to the outside, and to the Corporate WAN.

This topology is not secure and leads the implementers into a false sense of security. The main reason for the sense of security is that security policy and configuration is being implemented in the same manner as a traditional IT Network.

Control system networks, by definition and function, are used in almost opposite ways from machines installed in the business environment.

Defining the Secure Process Control Environment

Looking at what the control system is (what it does, what its intrinsic value is, and what its requirements are), we can easily see that traditional IT security techniques imposed on the system impede operability and functionality. The cumulative effect is that continual problems arise in keeping the control system running reliably.

Standard IT security techniques and strategies are not only minimally effective, but can be reckless and dangerous when applied to Control Systems. This is because IT practitioners apply standard techniques and strategies in the production environment.

Recall that the machine functionality between a Standard IT BusinessNetwork and a Control System Network is virtually 180° in opposition. Elements of the two network types look virtually identical, (machine hardware also looks identical when viewing from a high level), but that is where the similarity ends.

The functionality and operation between the two network types are wholly different and are not directly or desirably compatible without appropriate security and/or proxy interfaces.

When implementing security for the Control System environment, determine the following:

- What the total environment accomplishes.
- How it accomplishes the tasks it is assigned.
- What might be done to appropriately protect the system, while assisting or improving system and process efficiency.

Note For detailed information on assessing the Secure Process Control Environment, see Chapter 2, "Defining ICS Security Risk Areas."

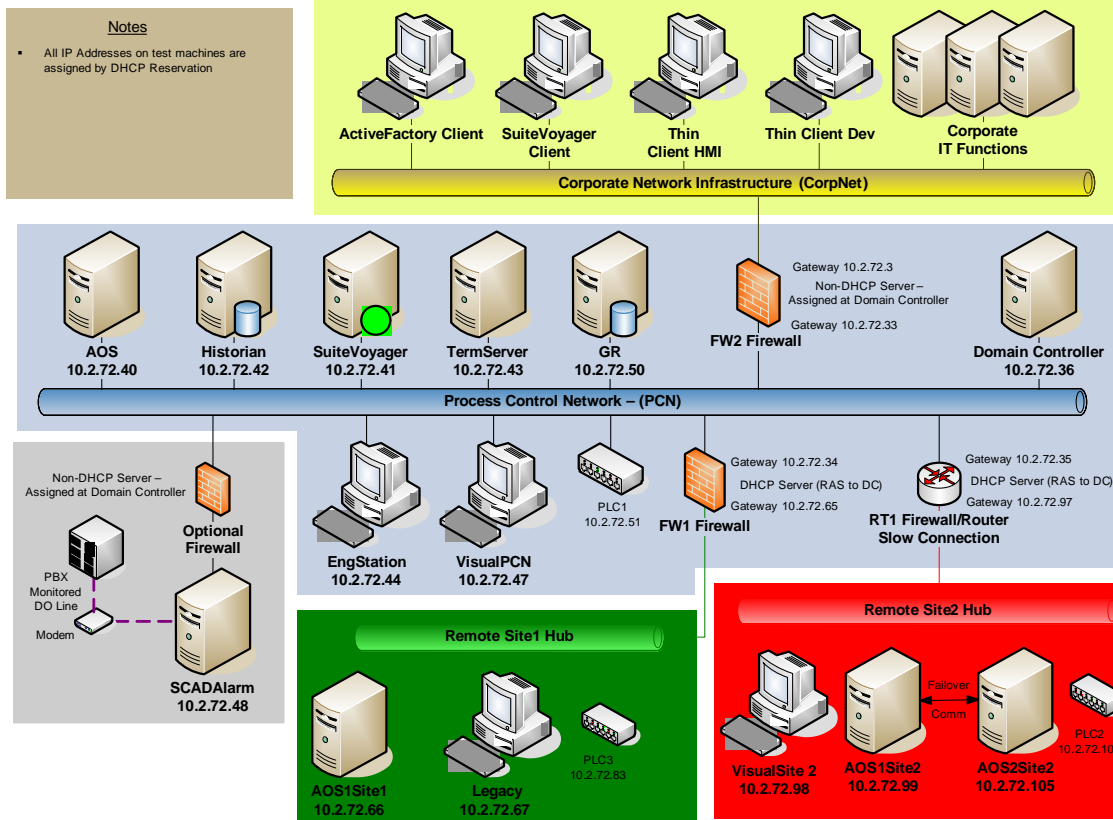
Defining the Layered Security Model

Industry guidance and policies state that machines have to be buried in layers of security, and this statement is essentially correct. However, implementing traditional security guidance policies in a control system environment is difficult, and ultimately counterproductive.

Current industry guidance shows several areas of high security with lessened security requirements in areas that might break the functionality of the system. This guidance is highly fragmented, and completely discounts the operation of the Process Control or SCADA System functionality in favor of a belief about what might be secure.

Therefore, a systemic approach should be used when reviewing Process Control Networks and SCADA System Environments. We can no longer look at individual machines needing a particular security profile without it affecting the entire Enterprise. To accomplish adding security to such an environment, it is necessary to apply security as experts recommend, but with an addition: Only one point of ingress/egress to/from the Control System.

ArchestrA Secure Reference Architecture Recommendations– Layered Security



As can be seen from the graphic, this security model addresses security on a systemic basis.

However, each bloc contains both secured and unsecured devices. In the previous graphic, unsecured devices are PLCs in each bloc.

Both device types are still vulnerable to everything that appears on the Corporate Net. Any virus, worm, DoS, MiM attacker, botnet, loss of domain control, IT Security change, automated OS update; basically anything can get into this system.

As a result, and rightly so, an IT person will state that they must install all sorts of countermeasures on the machines and close off ports and functionality and on and on. All these installations disrupt the functionality of any control system. The ongoing administrative overhead on this system is nearly unmanageable.

As IT personnel are likely to want to run third party software according to this architecture, it is also likely that such software will displace the machine's primary function. This software has been demonstrated to stop processes and disrupt data flow in certain circumstances.

Additionally, there is one outstanding problem with this architecture that makes it almost completely and uniformly undesirable and it is that Control System networks are seldom laid out so neatly. Normally, parts of a control system may reside in a remote location across a sub-domain, an unsecured WAN, or an Internet connection, which leaves it further vulnerable to attack and infection.

The OSI Model and Securing a Control System

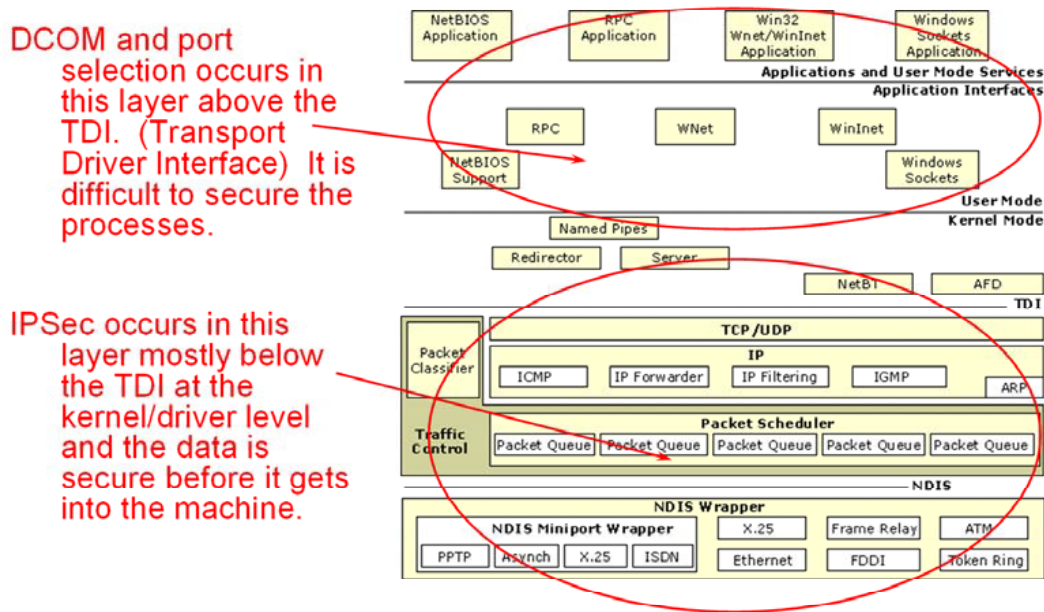
OSI (Open Systems Interconnection) is a standard description or "reference model" for how messages should be transmitted between any two points in a telecommunication network. Its purpose is to guide product implementers so that their products will consistently work with other products.

The reference model defines seven function layers. The functions take place at each end of a communication.

OSI is not always strictly adhered to in terms of keeping related functions together in a well-defined layer. However, many, if not most products involved in telecommunication make an attempt to describe themselves in relation to the OSI model. The model is also valuable as a single reference view of communication that provides a common ground for education and discussion.

The OSI model visualizes how a computer communicates and operates. The idea behind the OSI model is that when two computers communicate on a network, the software at each layer on one computer assumes it is communicating with the same layer on the other computer.

The following graphic describes the OSI model:



Transport Driver Interface

Note that the graphic includes a line separating the operation of the hardware and the operation of the software. This dividing line is called the **Transport Driver Interface (TDI)**. Software applications and most of the accessible parts of the OS are located above the TDI. Hardware interface drivers, firmware, and the BIOS exist below the TDI.

Security Changes Above the TDI Line

The operation and behavior changes made by IT groups are made only in the highest levels of the machine—The Application and OS Layers. Running AntiVirus software or any machine monitoring or VPN software clients in this layer will necessarily steal operating system resources, and preempt any primary function of the machine.

The model also shows that port closure (a technique that IT personnel are trained to use to limit functionality of a machine) also changes (disrupts) the Primary Purpose Applications, which also run in this layer.

Remember that other machines communicating with these applications on the machine must (by definition) pass through these artificial filters. The problem here is that IT personnel are likely to assume that a specific application does not need a certain (port range or) port, and close the port based upon a subjective determination of how they expect the primary-purpose software to run.

In practice, making any changes to this layer (without fully understanding why the functionality exists or is required) will change applications' behavior, sometimes causing unexpected results.

How Changes Effect the Control System Environment

In a Control System environment, port closure techniques very often break the designed functionality of the software. Remember that Control System Software is designed to operate in a Parallel Computing Environment. Changing any functionality within this layer will also change how that layer behaves toward any other machine trying to reach the application residing in that layer.

To exacerbate this problem, the common (incorrect) practice is that port closure will stop viruses and worms, because a certain number of them are designed to use specific ports. Unfortunately, botnets can search through various ports until it finds something it CAN communicate through, and then this port is used instead. It is even possible to pass this malware through Port 80 if that is the only port left open.

Note Changing or closing ports indiscriminately is called "Security by Obscurity," and thanks to the latest automated tools-- most of which are freely available to attackers-- this model is obsolete and ineffective.

Security Changes Below the TDI Line

The solution is to push machine security configuration down to a layer that does not have access from the application layer. This means that security enforcement should take place near the NIC hardware in the driver- or kernel area. This establishes a security perimeter around the entire ICS that very few individuals and processes have access to. In other words, the attack vector surface area for the ICS has been reduced to a very manageable level.

Enforcing security at this level also means looking at security in a different way:

Operations in a control system are designed to be steady-state and predictable. All machines are designed by intention to operate within a Parallel Computing Environment. Securing such a system with these trusted machines means, by definition, creating a secure area in which this Parallel Computing Environment can safely exist.

That is why establishing the secure perimeter below the TDI makes perfect sense. Looking at the model and reviewing all the transport interfaces that can be used, we can see that IPSec exists in this layer. By definition of the OSI model, this layer is expecting to communicate to other machines only at this level.

Using IPSec to Secure Control Systems

IPSec, or Internet Protocol Security, is a secure protocol encrypting standard TCP/IP packets with an encryption key known to the sending and receiving machines. IPSec provides aggressive protection against private network and Internet attacks through packet encryption.

Machines on the network *not* trusted in this environment cannot see or communicate with the secured machines. In other words, it is not possible to see or browse to any secured machine in any manner.

IPSec Communication Modes

IPSec is OS-independent and has two modes: **Transport Mode** and **Tunnel Mode**.

- **Transport** mode is used to establish communications between all the machines in the Enterprise.
- **Tunnel** mode is used to establish tunnels to unsecurable devices, such as PLCs and "Smart" Objects holding an IP address.

IPSec in the Business System Environment

IPSec is used in the Business System Environment to ensure secure communications between nodes using the **Transport** mode. In that context, IPSec is used to create secure domains within a larger network (Domain Isolation).

Note For more information on Domain Isolation, refer to [Improving Security with Domain Isolation](#).

IPSec in the Control System Environment

IT departments don't always address security on control devices, even though some manner of PLC or controller is the heart of every control system. Man in the Middle (MiM) attacks can still occur against the control system, or if nothing else, initiate an attack against the PLC directly.

Since instructions for forcing many of these devices into an administrative mode have been published on the Internet, attackers can attempt attacks against PLCs without your awareness or knowledge until damage has been done.

Control System security is configured using a similar concept to the "Domain Isolation" practice by using both the Transport mode, and the **Tunnel** mode for unsecured devices (such as PLCs) by placing a VPN Endpoint appliance (usually a small Endpoint Router) in line with the PLC.

Using IPSec allows the Control System Enterprise to live entirely within a larger Corporate WAN without anyone knowing it.

IPSec Benefits

The following list explains some IPSec configuration benefits:

- It is impossible to browse, write to or read any machine in the Control Enterprise unless you are a trusted machine.
- No ports need to be closed.
- No Services need to be stopped.
- Every product or module that is tested on a standard network will also work on a secured network.
- The data, telemetry, and control information are unencumbered by packet broadcasts and multicasts.
- Ping can also be disabled if desired.
- This secure PCN "bubble" can exist, with careful engineering, inside a larger Corporate Network or WAN, and no one will be any the wiser, except the trusted machines and administrators.
- Ongoing IT administrative overhead is reduced significantly.
- Enables visibility as Single Endpoint Device with a single point of ingress/egress.

When the Control System is isolated so effectively, with a single point of ingress/egress, it is possible to implement and enforce industry guidance of layering security around similar devices.

Future Outlook for IPSec and the Secure Perimeter

Note that as rootkits get more sophisticated in the future, it may be theoretically possible to violate device drivers and so open a new attack vector that previously did not exist. Rootkits have created a new, as yet unexploited, vector of attack that is fundamentally different than previous attack vectors. Rootkits currently enter a target at a high (on the OSI model) level and position the poisoned code into normal system modules at the next lower level, like an executable or system file like winlogon. Once established at that layer, a rootkit might then theoretically proceed to the next layer down in the OSI model on the local machine and poison a device driver, which does include IPSec (as a virtual device) creating a theoretically invisible hole in the perimeter.

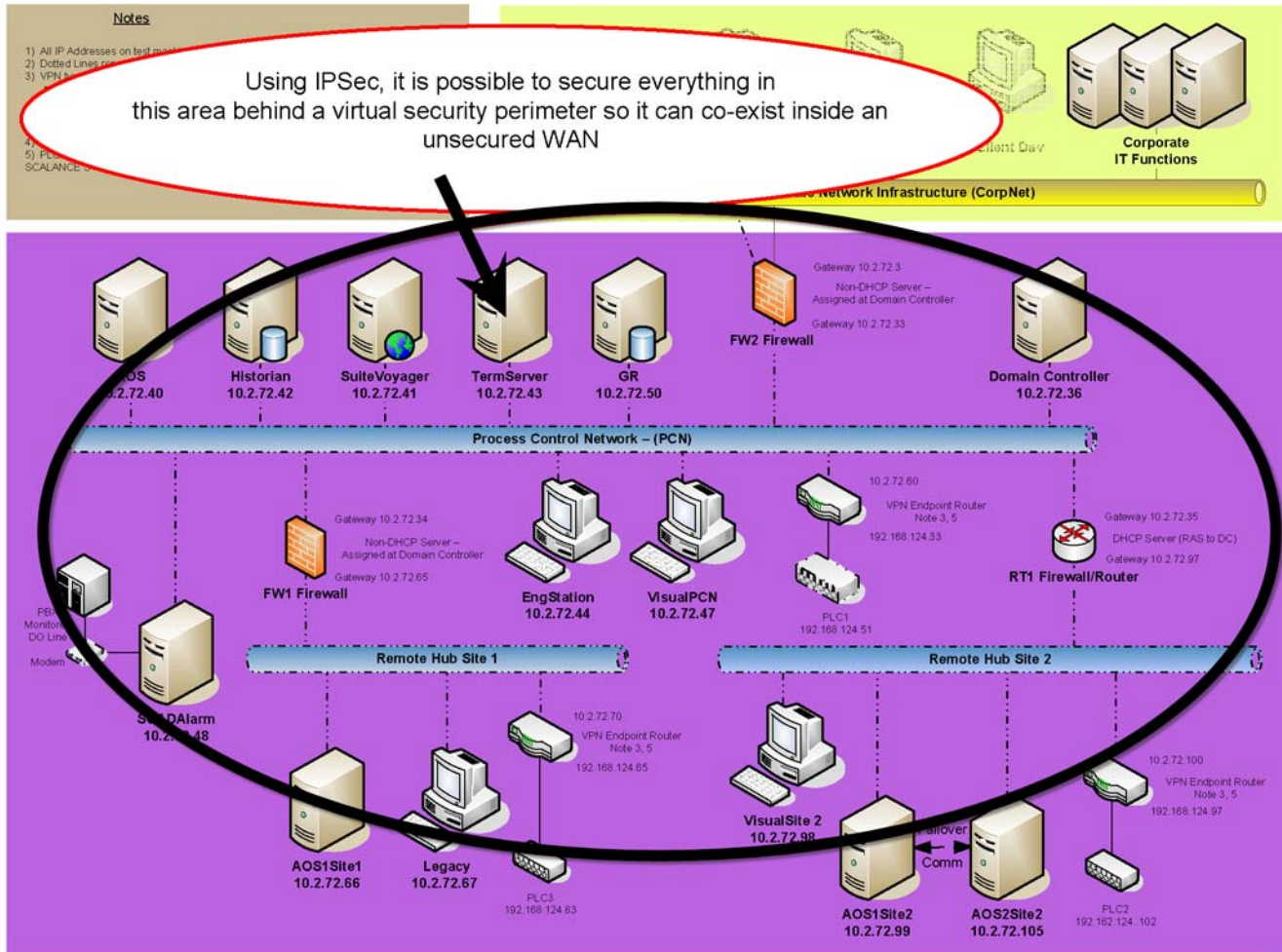
Therefore, it becomes very important to know what data flows into the ICS through a security perimeter established using IPSec. Local machine scanners (antivirus, anti-spyware, etc.) as we now know them will become increasingly resource hungry and also increasingly useless as time goes on because they operate above the layer that the poison code could infiltrate. The only theoretical counter for such an attack vector (at this time) would be absolute control of the data coming into the ICS, meaning an Active Intrusion Prevention System and limiting the data coming into an ICS only to what the system can interpret fully.

Configuring IPSec in the Single Endpoint Device

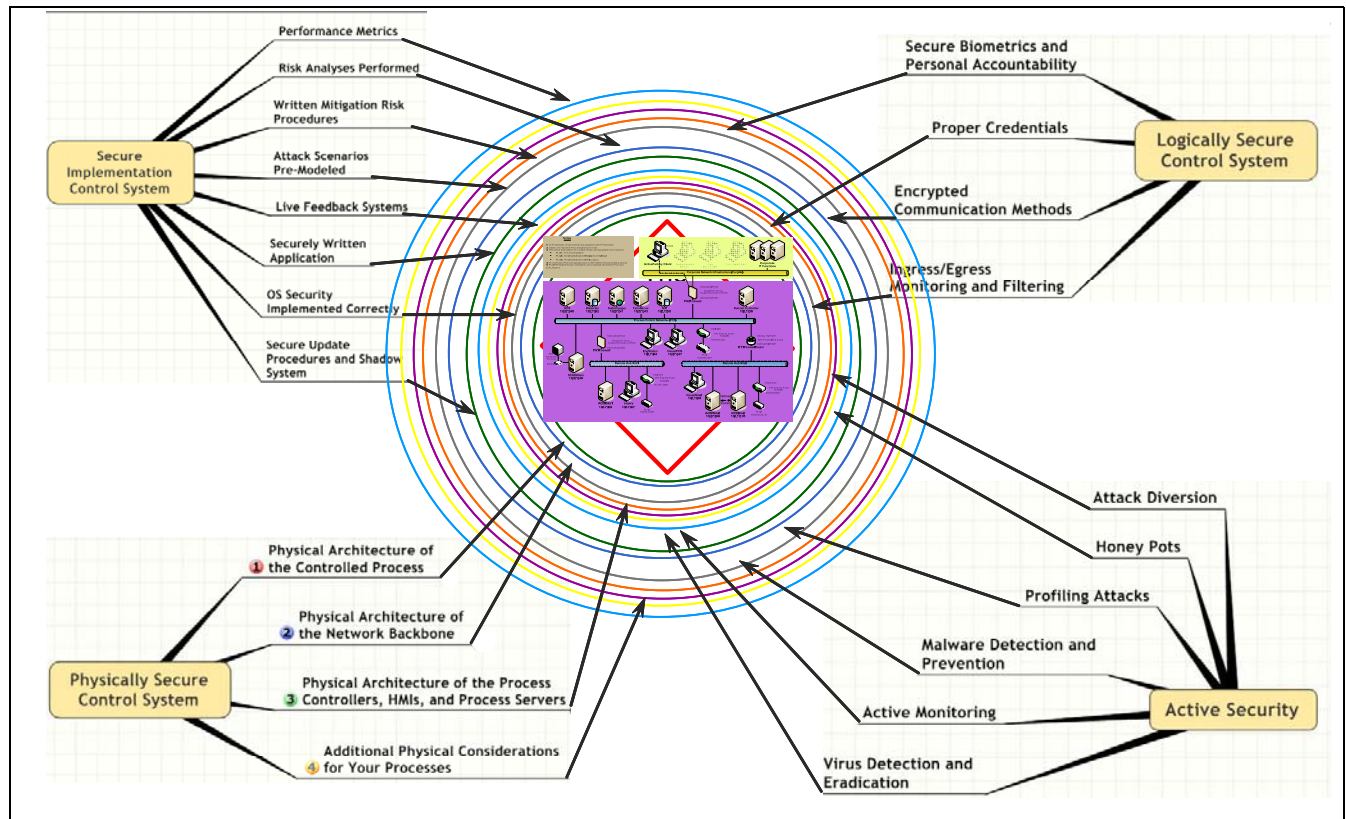
When the Control System is completely isolated behind a security perimeter, it can be viewed from an IT perspective as a Single Endpoint Device with a single point of ingress/egress. Security can be applied in a systemic manner and is much more effective.

The following graphic demonstrates this perspective.

ArchestrA Secure Reference Architecture Recommendations – Level 1.0 Security Applied



The following graphic represents the entire control system as the Single Endpoint Device from the IT perspective:



When the ICS is surrounded by a security perimeter, control for ingress and egress can be tightly maintained. Additionally, other disparate layers of security can be easily added outside the perimeter that create conditions for setting traps, logging surreptitious behavior, and observing anomalies in the Secure PCS operation, which can be used as alarming triggers in much the same way that SPC (Statistical Process Control) operates.

Note Without first establishing a security perimeter incorporating people, policies, processes, and products, any attempt at proactive security is futile.

IPSec Configuration Notes

The following IPSec functionality must be analyzed in the planning stage. Detailed configuration information is included in the following chapter.

IPSec Off-loaded Processors

Ensure reliability of the IPSec layer by off loading the encryption/decryption processing from the main machine processor.

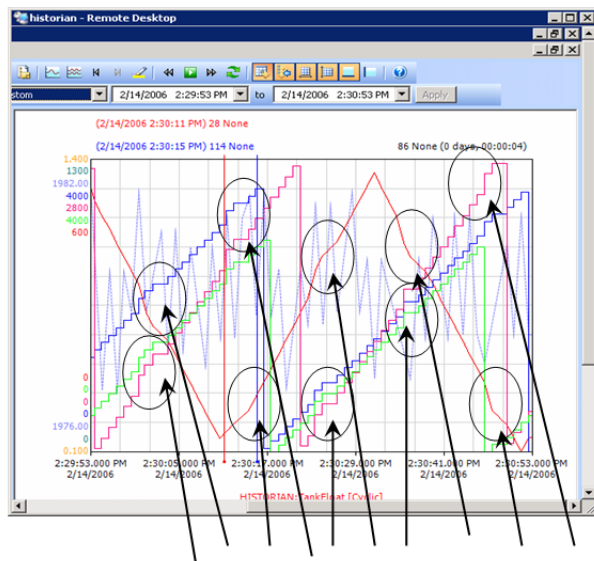
Several companies manufacture a NIC (Network Interface Card) with a dedicated co-processor used to negotiate security. At least one manufacturer also has placed a centrally managed offboard firewall system on each NIC as well, and if dedicated machine firewalls will be used in the system, it is advisable to purchase these devices.

An important benefit of using the Off-loaded Processor is that process data flow will not be interrupted by IPSec negotiation, as it would when using a shared processor.

Note that it is not a requirement to use IPSec co-processors. The ability to utilize IPSec is already built into the NIC and the OS. Coprocessors may be required however if machines are heavily burdened with ongoing ICS processing duties and do not have the bandwidth to include encrypting and decrypting the IPSec packets. Machine resource problems can be detected early by looking for delayed or missing network packets, which translate to missing production data. Careful monitoring of the machine resources in a steady-state normal-operation scenario will uncover if the coprocessor NIC is actually needed.

The following graphic shows a comparison between non-off-loaded processor performance, and off-loaded processor performance on a slow machine (800 Mhz) that is running an HMI and IOServers concurrently. Note that DAServers, which operate within a different process thread, do not seem to be encumbered by the encryption and decryption processing. This particular machine was averaging 40% steady-state primary-purpose resource utilization and peaks occurred in processor usage that went to about 100% when certain IPSec maintenance processes were performed by the OS (as opposed to the co-processor NIC).

OS Handling IPSec Negotiation



IPSec Negotiation Offloaded to NIC Co-processor



Circled items are IOServer Data where Server was halted during IPSec Negotiation. Note that DAServer data (dotted blue in background) are unaffected.

IPSec Transport Mode

IPSec **Transport** Mode is the basic connectivity mode that is used to connect various Windows machines within a Process Control "endpoint device."

Using IPSec Transport, it is possible to secure Windows Machines in the production area so they can co-exist within a secure PCS inside, an unsecured WAN.

IPSec Tunnel Mode

IPSec **Tunnel** mode is used for PLCs, "Smart" devices that have an IP address, and legacy SCADA equipment that attach to the Secure PCS enterprise through Ethernet or IP connectivity, because they are unsecured devices, and therefore operate on an "untrusted network." IPSec Tunnel mode configures the communication tunnel between a configurable IP start- and end point.

Tunnel mode is normally used for secure "site-to-site" communications over an untrusted network. Each site has an IPSec gateway configured to route traffic to the other site. When a computer in one site needs to communicate with a computer in the other site, the traffic passes through the IPSec gateways (and possibly through intervening routers in each site before reaching the local gateway). At the gateway the outbound traffic is encapsulated inside *another* complete packet and secured according to the details of the filter action defined in the Security Rule.

Note Defining filters and Security Rules is explained in Chapter 6: Configuring IPSec and Domain Isolation for the ICS Environment.

Of course, the gateways have already performed their "Phase One" authentication, and established their "Phase Two" signing/encryption security association.

Note In IPSec for Windows Server 2003, tunnel mode is supported only for site-to-site VPNs on Routing and Remote Access Service (RRAS) gateways and not for any kind of client-to-client or client-to-server communications.

VPN Endpoint Devices

VPN Endpoint devices (PLCs and "intelligent" objects with an IP Address) are used with a proxy or "translator" to convert between TCP/IP and IPSec. These proxies are nothing more than simple VPN Endpoint routers.

Many types of VPN Endpoint appliances are available. All of these devices do the same thing—basically sit in front of an IP device as a "bump in the line" and translate incoming IPSec into usable IP packets that the PLC or unsecured device can understand.

Defining the ICS Security Layers

Alternatives to VPN Tunnels for Unsecurable Devices

New appliances are currently being designed that are basically an encapsulated VPN tunnel (invisible to the user) with an internal Linux operating system that could be used to simplify configuration complexity and maintenance overhead. Additionally, at the time of writing, other, different devices are currently being tested and developed that may be able to present an IPSec Transport mode "face" to a Windows isolated domain that would be installed directly on the network ahead of an unsecurable IP device instead of a VPN endpoint described earlier. Such a device would greatly simplify configuration of large ICS Enterprises, so that there would really only be two security rules on each machine. Before committing to purchasing any appliances, you should check the current level of technology that is available since it changes very often. Simplicity is the key to creating a secure perimeter and environment. It may save you much time, money, and future problems.

Introduction

Creating security within control systems can be a daunting task. In order to fully implement ICS security correctly, it is important that security, as previously mentioned, encompass People, Products, Process, and Procedures. Not addressing any of these areas in conjunction with the others may leave extremely dangerous threat vectors to the secure system. For instance, applying the techniques described within this section may expose the whole enterprise to vulnerabilities if proper social engineering has not taken place to clear and train personnel for proper use of the Secure Control System.

Microsoft has recently begun describing "domain isolation" as the security model of choice that is based on work done within the Control System Industry. Domain Isolation will be used extensively within the Vista/Longhorn and future platforms, and is currently available as an easily installed option within XP/Win2K3 with the release of Hotfix 914842. It is not recommended to apply the isolated domain model to a Win2K network as it is extremely difficult to configure, and tools to check configuration and health are either poor or non-existent.

Microsoft isolated domain techniques have been described by Wonderware as the "Secure Process Control System," or "Secure PCS" and these terms may be freely interchanged when discussing ICS security. In addition to the information offered by Wonderware in this document and in the online classes and seminars, there are currently classes given by both the ISA on Encryption and VPNs, and by Microsoft on creating the virtual security perimeter or "bubble" of the Isolated Domain or Secure Process Control System.

This chapter defines and describes 5 Security Levels:

- **Level 0:** Uses the Simple Layered Security Model (SLSM), which has previously been described in this chapter as the minimum standard industry security model with no perimeter security.
- **Level 1:** Uses IPSec Transport and Tunnel Modes to establish a known security perimeter around the ICS in order to create a truly secure Isolated Domain. Some industries also call a small subset of this security technique, "Automation Islands".
- **Level 2:** Uses offboard Firewall processor technology to augment IPSec to create an optional secondary layer of security above IPSec but still below the application and OS layers in the OSI Model. This is an ideal location for a second security perimeter, because it has a very small "surface area" in regard to attacks and very few people have access to it.
- **Level 3:** Uses Secure Routers to augment the previous Security Levels and isolate any force-connected possible external threat vectors (such as an unpatched notebook) into a separate isolated domain.
- **Level 4:** Uses Secure Gateway Devices and stateful firewalls to augment the previous Security Levels by filtering the single point of ingress/egress into the Isolated Domain using a Realtime Active Gateway Filter.

Defining and Establishing Level 1 Security

Level 1 security is considered the minimum secured environment in which a Process Control Environment or SCADA System should be operating.

Level 1 Security: Establish the IPSec Security Perimeter

Setting up domain isolation or the Secure Process Control System requires advance planning.

High-level recommendations include:

- Plan out well ahead how you will deploy the changes.
- Use a spreadsheet to assist in rules definition/configuration to help eliminate configuration errors (mostly during VPN rules design.)
- Get your VPN Monitoring (and other IT Tools) ready to use.

Detailed recommendations are explained in the following sections.

Note The recommendations are designed to be implemented in the order they appear here.

Install the OS Without Security

One of the biggest mistakes made when implementing a Control System is attempting to install its components on a network of machines that include pre-defined security templates. This practice has cost many customers months of additional integration time, troubleshooting issues that they created themselves.

Over 15,000 Active Directory rules can be applied to any single machine in the Process Control Network. Applying the wrong rule ahead of time can actually prevent installing and correctly configuring the Control System.

Many security settings are undefined by default. After defining a security rule that breaks the Control System, there is no way to "undefine" the rule. The only recovery solution is to reinstall the operating system on the affected machine(s).

Installing the OS without security ensures that all the machines in the peer-to-peer Parallel Processing Environment are working together. Until this condition is satisfied, it will be impossible to review the effects of the application of any security template.

Check Connectivity to Machines and Devices

Ping and browse to all machines at this point in the configuration, before any application software is installed.

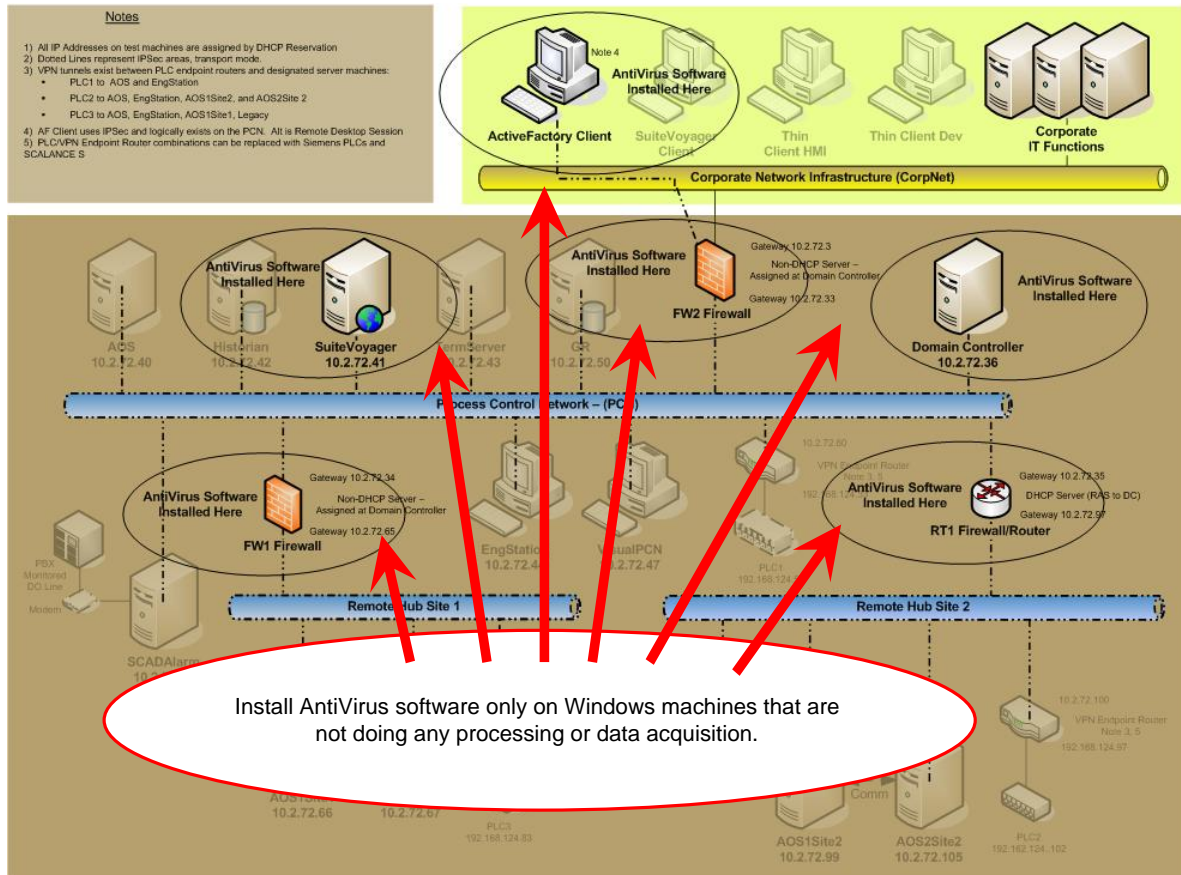
To check communications with the PLCs, use the PLC development software installed on your Engineering Station. The Engineering Station should be one of the tunnels established to each PLC. This step verifies the operation of the VPN Tunnels and Endpoints.

Install AntiVirus / Anti-Spyware / Anti-Rootkit Software

The next step is to install the Anti-Malware Software that will run on any gateway or perimeter interface machines.

These machines can be classified as any node that does not process control information or data, but does somehow interact with the outside world.

The following figure shows Anti-virus software installed on the ActiveFactory node, Firewalls, Domain Controller, and SuiteVoyager nodes:



Configure IPSec Between Machines

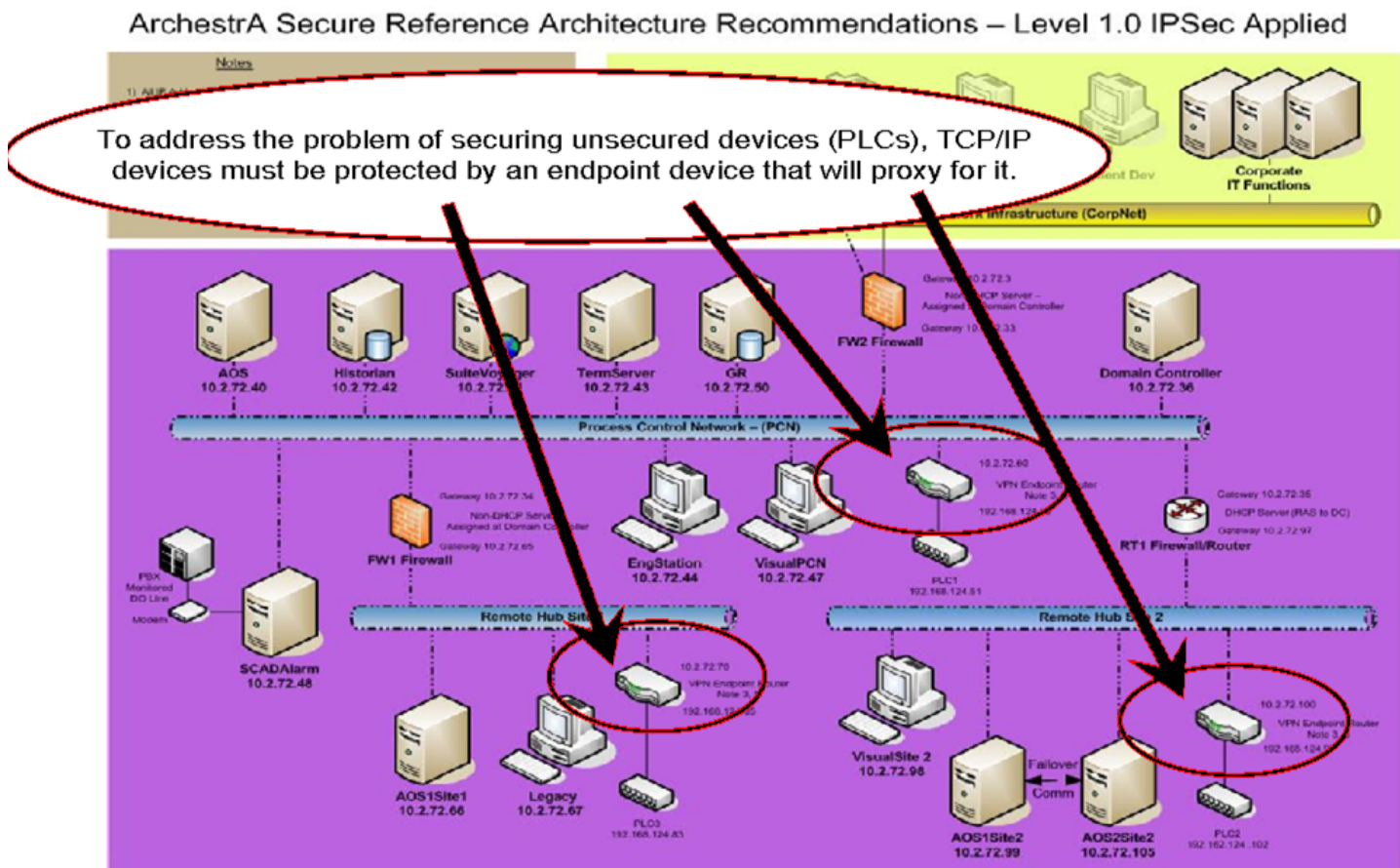
Configure IPSec **Transport** and **Tunnel** modes between machines and endpoint devices, respectively. See Chapter 6, "Configuring IPSec and Domain Isolation for the ICS Environment," for detailed configuration information and setup examples.

Using VPN Endpoints to Secure Unsecurable IP Devices

VPN Endpoints are nothing more than either a small router with this built-in functionality or a dedicated device designed with this functionality. These appliances are placed directly in line with, and physically in the same cabinet as unsecurable devices like PLCs and "Smart" objects such as IP switches and sensors.

These appliances become a proxy or "translator" for the unsecured device to "convert" between TCP/IP and IPSec. Many types of VPN Endpoint appliances are available on the market, and they all do the same thing-basically sit in front of an IP device as a "bump in the line" and translate incoming IPSec into usable IP packets that the PLC or unsecured device can understand. The physical appliance is generally locked in the cabinet with the PLC. The appliance is assigned 2 IP addresses, one for the unsecured device that is protecting and one for itself.

The following graphic shows the VPN endpoint devices as PLC proxies:



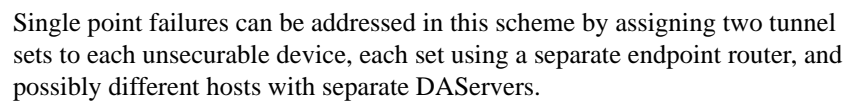
VPN Tunnels

Using these VPN Endpoints with the secured device requires configuration of tunnels from those devices to the machines that they will be communicating with. A tunnel must be defined for each individual machine it will be communicating with.

IPSec **Tunnel** mode is used to create the VPN tunnels necessary to secure devices that are not otherwise configurable for security. These devices usually are PLCs and "Smart" valves and switches. In other words, any device that has an IP Address, but does not have IPSec.

A tunnel must be defined between each individual machine pair, and one is necessary for each direction; in other words, two tunnels are necessary between machine pairs.

ArchestrA Secure Reference Architecture Recommendations – Level 1.0 VPN Tunnels



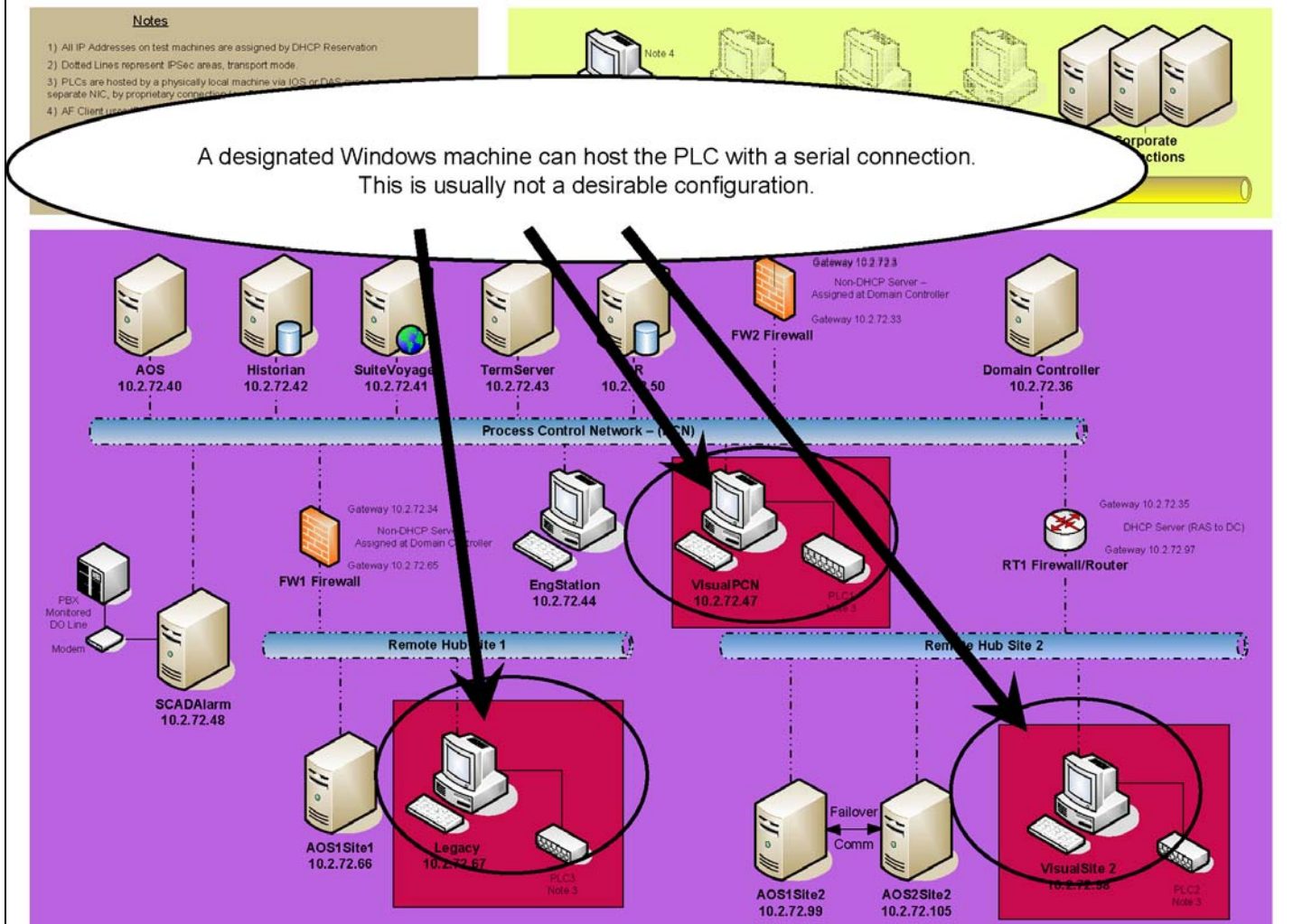
Using the PC as the Endpoint Device

It is also possible to use an ICS PC, such as a DAServer designated machine as an endpoint device.

The idea is to use the PC as an IO Server or DAServer host for the PLC, then use a proprietary method such as DH+ or serial connectivity to the PLC through proprietary hardware or an individual port in the PC.

This strategy is a simpler configuration but not desirable for reasons of access, cost, and/or single-point failure (which are not necessarily security issues). However, these methods of connection are a perfectly acceptable means of hosting and securing a PLC, and will lower enterprise configuration complexity considerably by not requiring the VPN tunnel configuration.

ArchestrA Secure Reference Architecture Recommendations – Level 1 Security Alternate



Recheck Connectivity to All Machines and Devices

Ping and browse to all machines at this point in the configuration, before any application software is installed. In order to check communications with the PLCs, use the PLC development software installed on your Engineering Station. The Engineering Station should be one of the tunnels established to each PLC. This will check the final operation of the VPN Tunnels and Endpoints.

Install the ArchestrA Framework

Install the Bootstrap, then deploy to each node. At this point, verify connectivity with the PLCs to their endpoint machines using ping and WWClient. When the system is deployed, that is all that is needed – the Control System is now running in a secure environment.

Level 1 Security Variations

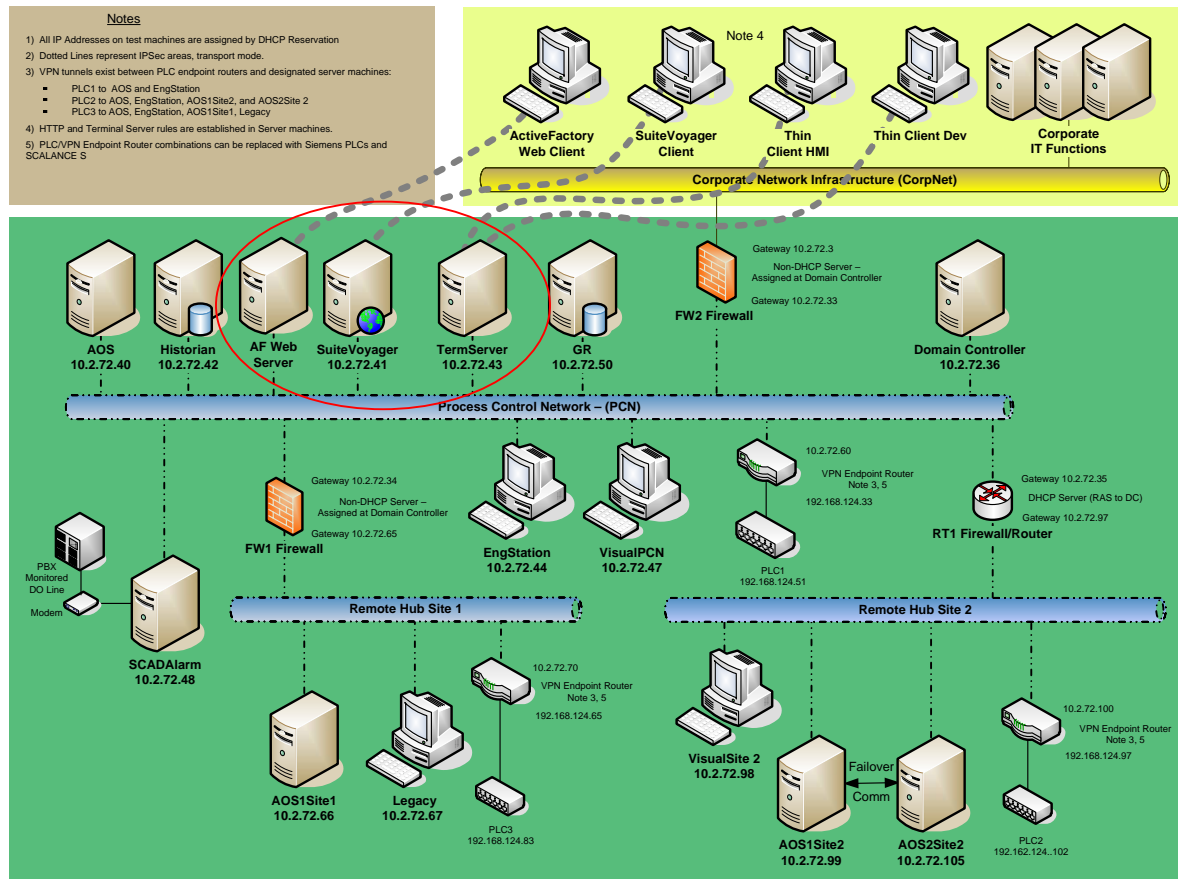
This section explains some variations to the Level 1 Security Strategy.

External Connectivity and Data Availability

It may be necessary to add secure variants and exceptions to any additional points of ingress/egress. For example, it may be necessary to open a firewall port for certain nodes. Mitigate the use of the open port to be consistent with your corporate security practices, which may involve a DMZ or proxies.

You may also want to secure the "outside" TS clients by bringing them into the subnet and applying IPSec.

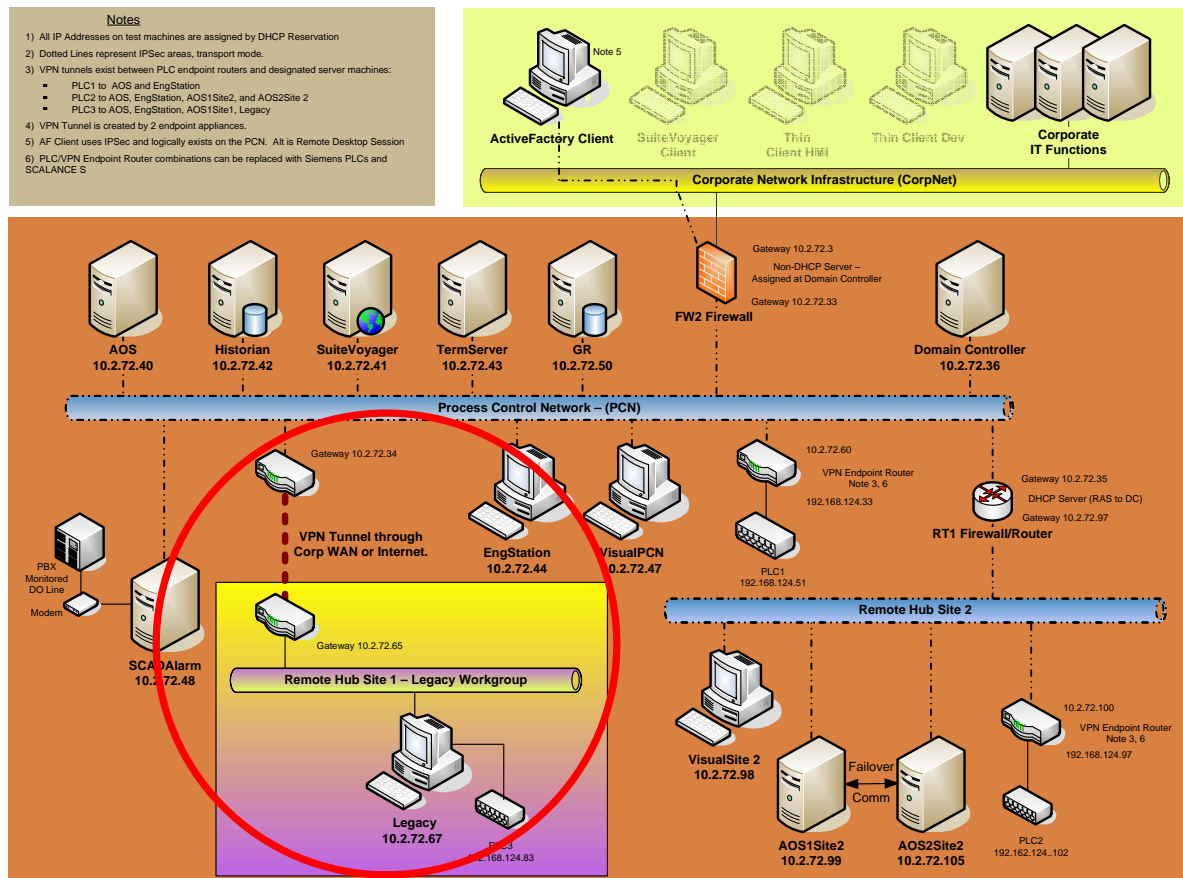
It is also advisable to secure any web clients by using Secure Sockets (HTTPS). The following graphic shows connections to AFWeb Server, SuiteVoyager, and Terminal Server nodes:



Establish VPNs to Legacy Workgroups

Depending on what functionality is included in the Control System, there may be legacy nodes that are HMIs and possibly IDAS. Connecting these within the secure environment through an unsecured WAN or a VPN appliance pair is possible.

The following graphic shows a remote legacy site connected via a secured gateway:

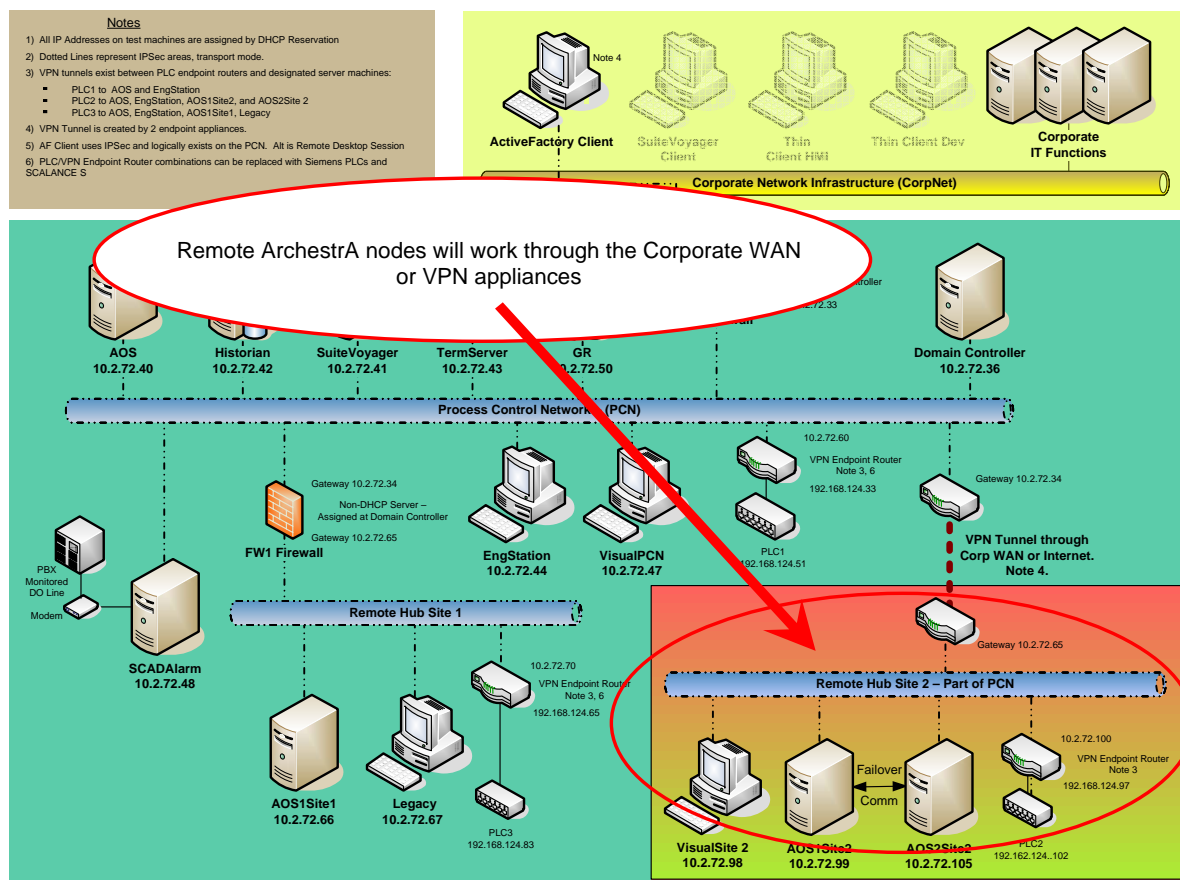


- Use a VPN device instead of software.
- A remote legacy site can be added even when using IDAS.
- Remote IDAS can be used by upgrading to the latest versions of InTouch and InSQL Server

Establish VPNs to External Enterprise Membership

Depending on what functionality is included in the Control System, there may be other Enterprise nodes that may be located in remote locations. It is possible to run the secured machines through a Corporate WAN or VPN appliances across the Internet.

The following graphic shows a remote location as a member of the Secure PCS Domain and a functional part of the ArchestrA platform. Two VPN Endpoint appliances can be used to establish a secure tunnel through an existing corporate WAN or even the Internet. Note that there are other VPN tunnels already established for PLC connectivity that can exist as a separate and unique tunnel *inside* the new tunnel created using two endpoint appliances.



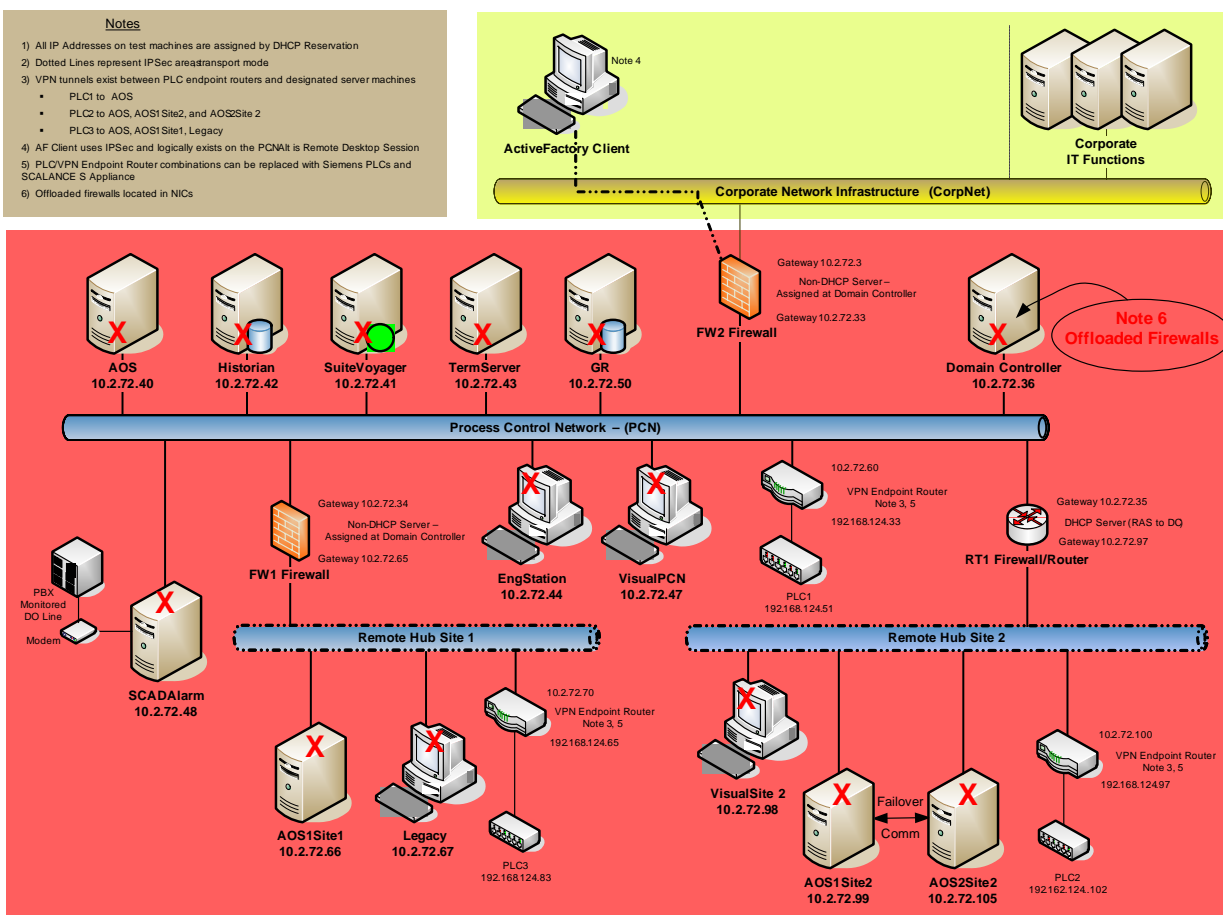
Level 2 Security: Machine-Level Firewalls

After establishing Level 1 Security on your Control System, additional levels of security may be required to satisfy various needs or requirements, and the addition of additional machine-level firewalls is recommended.

If the IPSec co-processor NICs also include an offboard firewall processor (such as the 3Com NIC), firewalls can be managed from a single site and do not exhibit a client interface on the local machine. Management can take place from a single point such as the Active Directory machine or Domain Controller.

Don't mistake this with the use of software firewalls. Software firewalls have unpredictable effects on the target machine and are difficult to manage in large numbers.

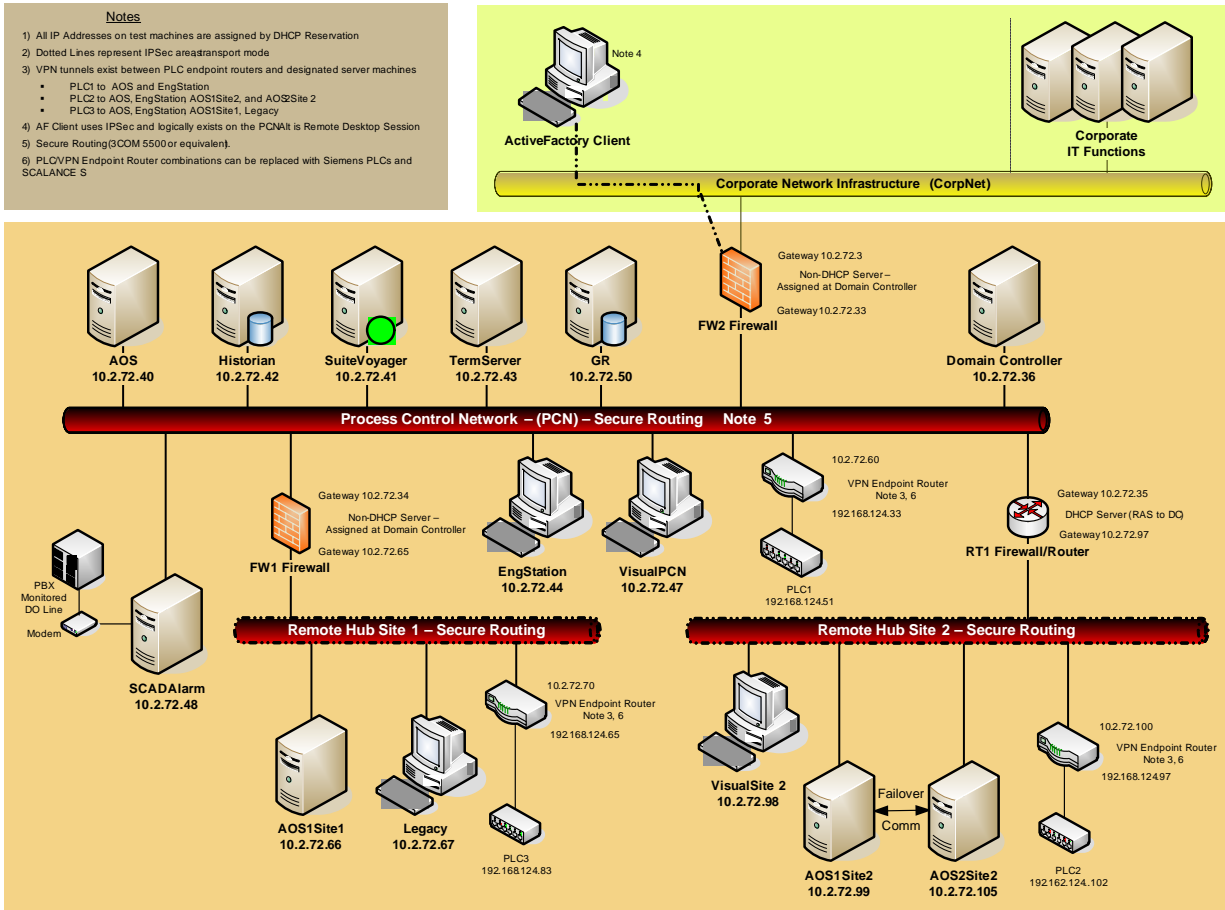
ArchestrA Secure Reference Architecture Recommendations – Level 2.0 Security Applied



Level 3 Security: Secure Routing

It is possible to secure the control system even further by using intelligent and secure routers such as the 3om 5500 series, Verano, ortinet, isco, et cetera secure routers. Foreign machines are placed into their own workgroups and it is impossible to connect to or see any machines within the securely routed environment.

ArchestrA Secure Reference Architecture Recommendations— Level 3.0 Security Applied



Level 4 Security: Secure Perimeter Gateway Devices

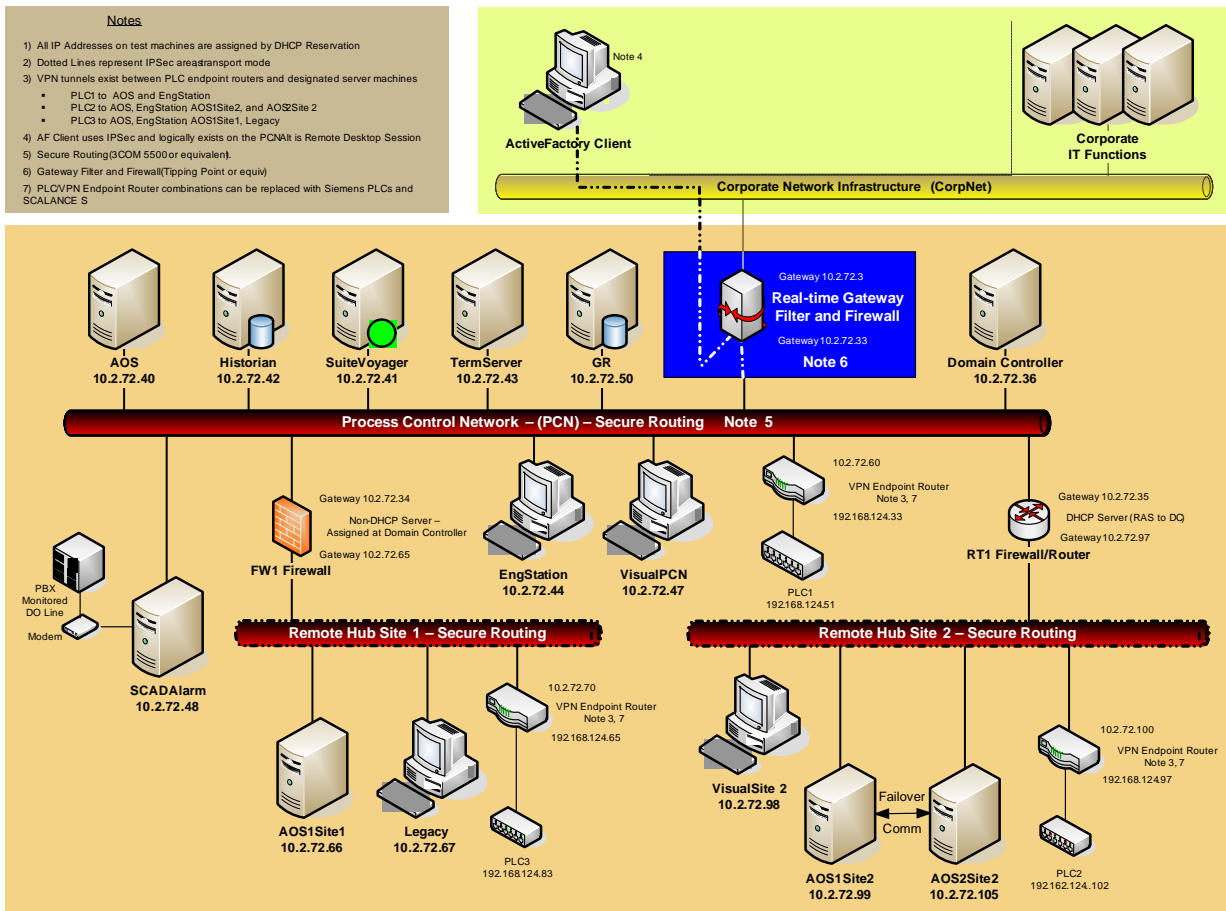
Since the ICS has now been established into a single entity (assuming that the security breach vectors of people, policies, procedures, and products have all been addressed and mitigated) that may exist independently or perhaps within a larger WAN, and only one point of ingress/egress has been configured, it is now possible to add another layer of security that filters real-time any data and communications through the secure perimeter.

The appliance is a combination firewall and router, along with a real-time Intrusion Detection System (IDS) / Intrusion Prevention System (IPS) engine that has current virus and OS security patch definitions built into it.

This means that if you have actually created an environment where there is only this one single access point, an entirely new security realm is available to use.

For example, it is possible to rely on the IPS/IDS gateway filter to perform the ongoing critical updates, virus definitions, and security patches. It is no longer necessary to install any of these updates on your secure PCS Enterprise until an appropriate maintenance cycle comes up. Additionally, new critical patches can be bench tested without the pressure of having to install them as soon as they are released. Security maintenance has now shifted from being "reactive" to being "pro-active".

ArchestrA Secure Reference Architecture Recommendations– Level 4.0 Security Applied



C H A P T E R 6

Configuring IPSec and Domain Isolation for the ICS Environment

This chapter provides configuration examples of a specific IPSec configuration within an Industrial Control System "endpoint device." The information covers the two IPSec modes (Transport and Tunnel) in detail, and provides a VPN monitoring example.

For more detailed information about using IPSec for domain isolation, how it works, and more details about how to configure it, see Appendix A, "References for more help and information," for several links to Microsoft IPSec and domain isolation websites and guidance manuals.

Warning: It is highly recommended that the setup shown within this chapter should be done by an MCSE Security certified Domain Administrator. Personnel who have not had the benefit of this particular training and experience may not understand key concepts of the Active Directory and domain isolation setup. Additionally, if your automation system is being certified or audited, it may not pass if you do not have the properly credentialed personnel establish the IPSec domain isolation security perimeter for the ICS/SCADA System.

Note Construction of the necessary rules and filters for your particular domain isolation setup may be substantially reduced by applying Microsoft Update KB 914841.

<http://www.microsoft.com/downloads/details.aspx?familyid=C44DFDA8-48AE-4868-89A6-67F7612ADFB1&displaylang=en>

Contents

- Configuration example of the IPSec perimeter for ICS
- Configuration example of the Organizational Unit (OU) for Machine Communication
- Configuration example of Unsecured Device Communication
- Monitoring the VPN Device

Configuration example of the IPSec perimeter for ICS

IPSec configuration is performed from the **Active Directory Users and Computers** Management Console (**dsa.msc**). Open the management console (on the Active Directory node) from the **Start/Programs/Administrative Tools** menu.

Note The following information describes an existing laboratory configuration (rather than showing empty dialog boxes), and is intended as a high-level roadmap. Administrator-level user with appropriate permissions is assumed.

Creating the Organizational Unit

Organizational units are Active Directory containers into which you can place users, groups, computers, and other organizational units. An organizational unit is the smallest scope or unit to which you can assign Group Policy settings or delegate administrative authority.

Using organizational units, you can create containers within a domain that represent the hierarchical, logical structures within your organization. You can then manage the configuration and use of accounts and resources based on your organizational model.

Organizational units can contain other organizational units. A hierarchy of containers can be extended as necessary to model your organization's hierarchy within a domain. Using organizational units will help you minimize the number of domains required for your network.

You can use organizational units to create an administrative model that can be scaled to any size. A user can have administrative authority for all organizational units in a domain or for a single organizational unit. An administrator of an organizational unit does not need to have administrative authority for any other organizational units in the domain.

Note No testing for "upper bounds" (number of supported Active Directory Organizational Units or their connections) has occurred. See "IPSec Configuration Best Practices" on page 241 for other implementation details.

This example describes two Organizational Units necessary to define a simplified IPSec Security model:

- **IPSEC REQUIRE No Tunnels:** Created to connect nodes within the Control System environment.
- **IPSEC REQUIRE Tunnels:** Created to link to designated PLCs or other unsecured devices.

Note The following section refers to the Organizational Unit as "OU." The steps included are not complete but are designed to enable an Administrator to create the necessary IPSec elements.

Configuration example of the Organizational Unit (OU) for Machine Communication

The following section provides configuration options for an OU designed for IPsec communication between Control System nodes.

Configuring IPsec Transport Mode

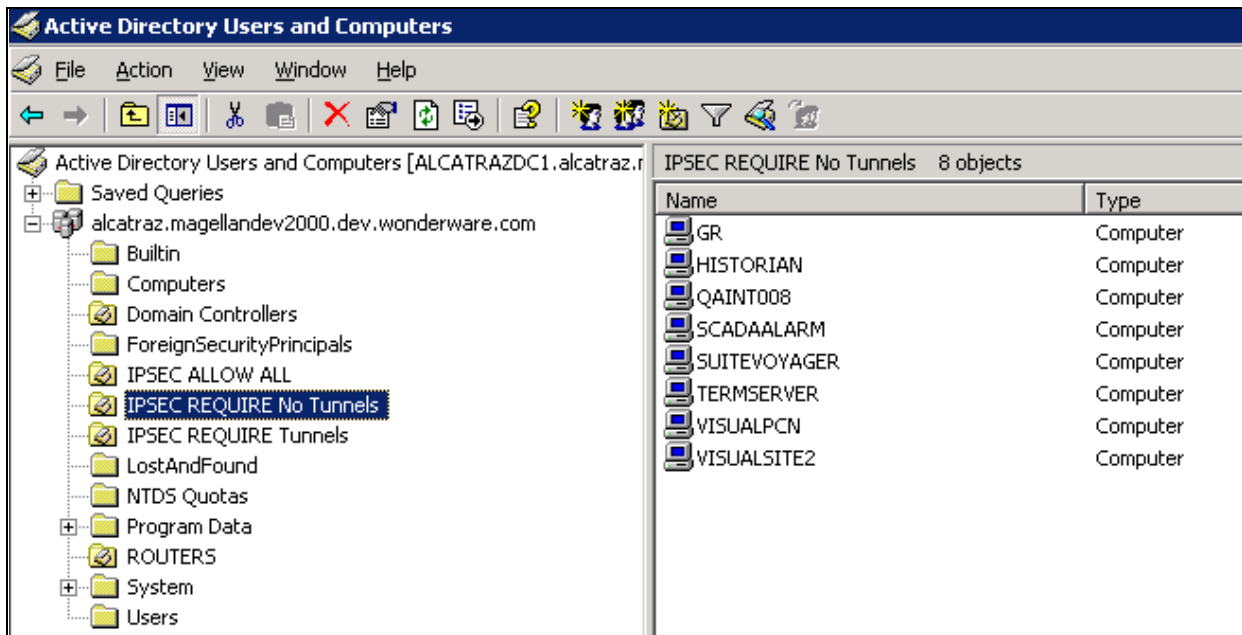
To ensure secure communication between machines within the "Endpoint Device" defined in the previous chapter, use IPsec Transport Mode.

To configure the IPSEC REQUIRE No Tunnels Organizational Unit

The Active Directory contains many OUs created by default. To create a new OU:

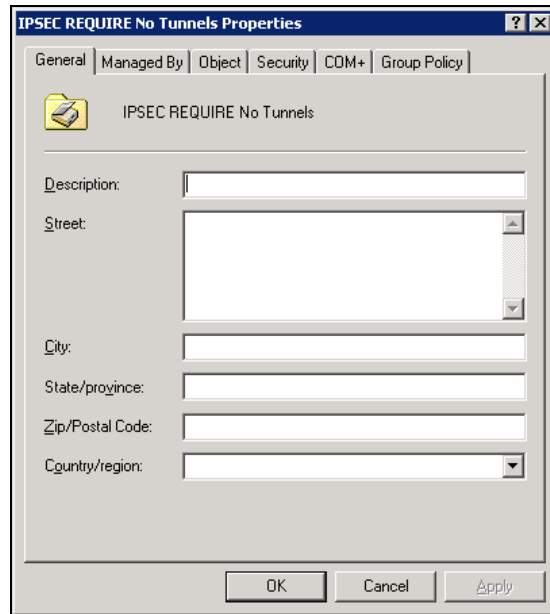
1. Right-click the domain name at the top of the hierarchy and select **New/Organizational Unit**.
2. Name the OU according to your security conventions. This example shows one OU created for "No Tunneling" and one for "Tunneling."

The following graphic shows the MMC and some sample IPsec Organizational Units:

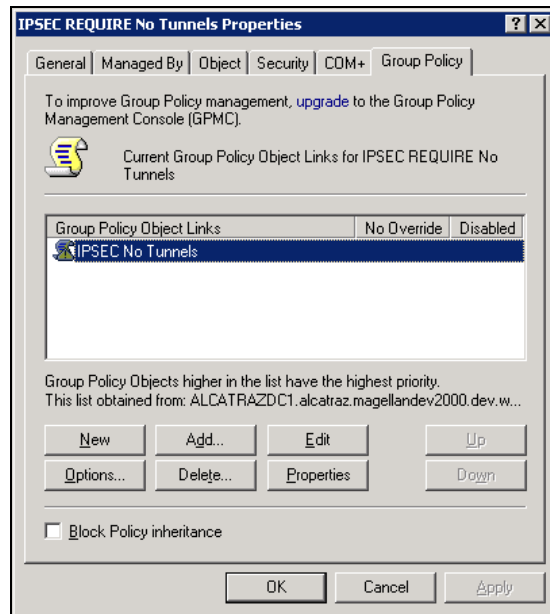


The following material focuses on configuring an OU that contains Security Rules for inter-node communication within the Control Network (IPsec **Transport** mode).

3. Right-click the **IPSEC REQUIRE No Tunnels** OU and select **Properties**:

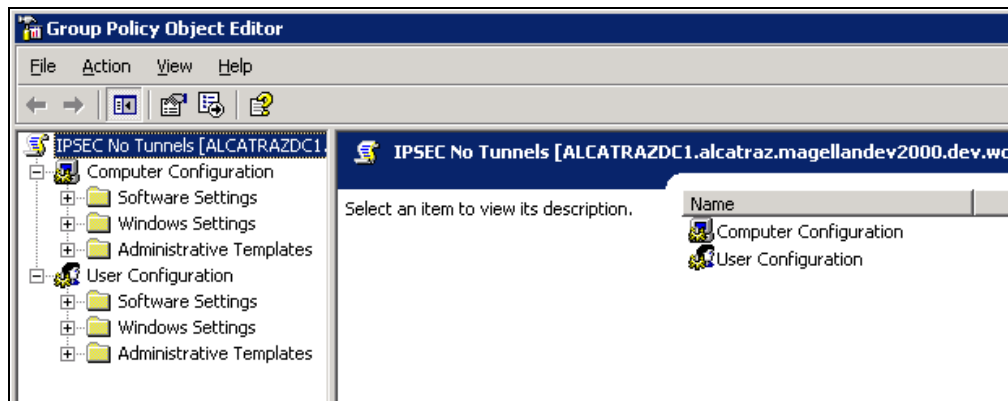


4. Select the **Group Policy** tab. In this example, a Group Policy has been configured. If a new Group Policy is required, select the **New** button:

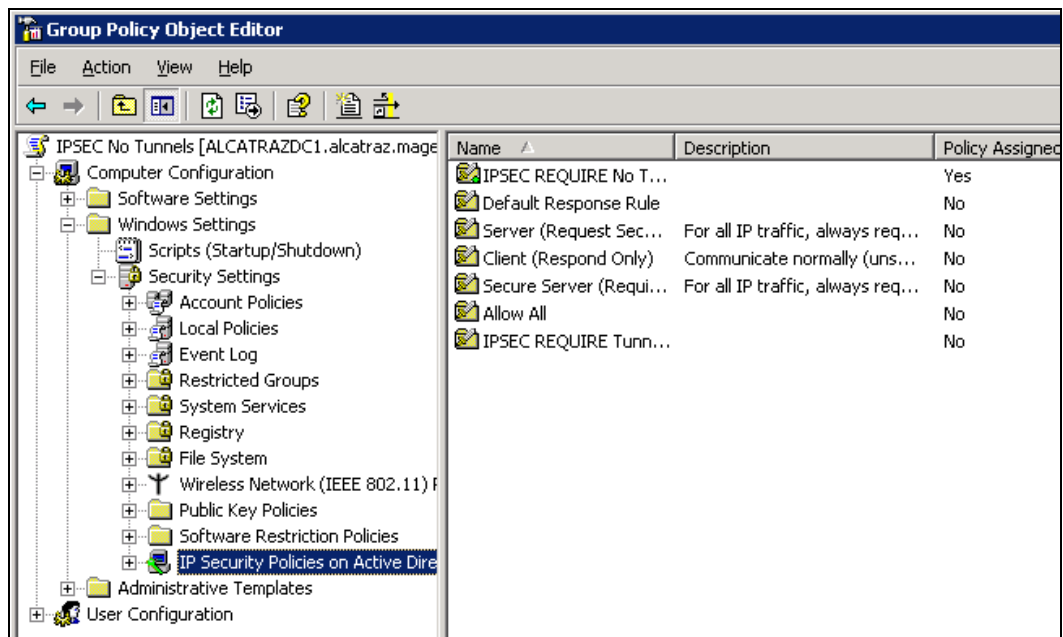


5. Click the **Edit** button to analyze the existing policy.

The **Group Policy Object Editor** appears:

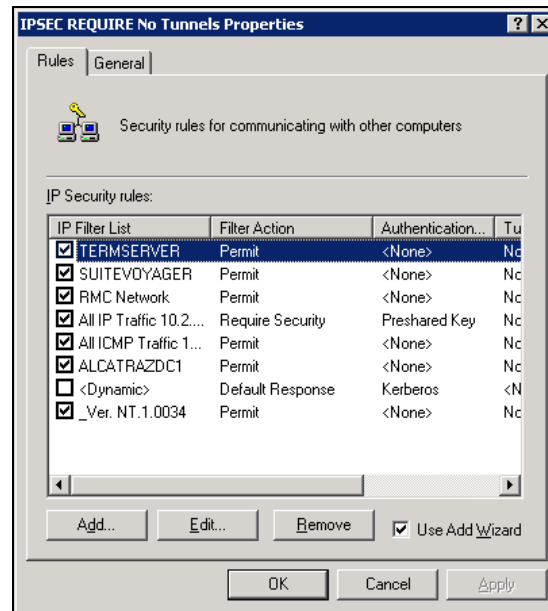


6. Expand **Computer Configuration**, then **Windows Settings**.
7. Expand **Security Settings**, then **IP Security Policies on Active Directory**:



8. Highlight and right-click **IPSEC REQUIRE No Tunnels**, then select **Properties**.

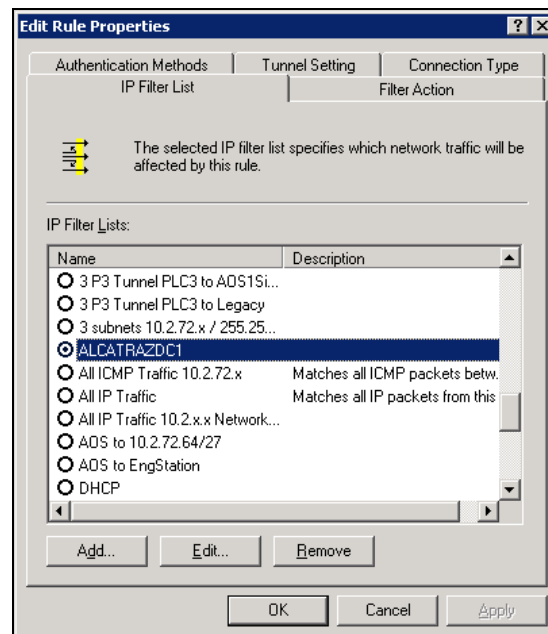
The **IPSEC REQUIRE No Tunnels Properties** dialog box appears:



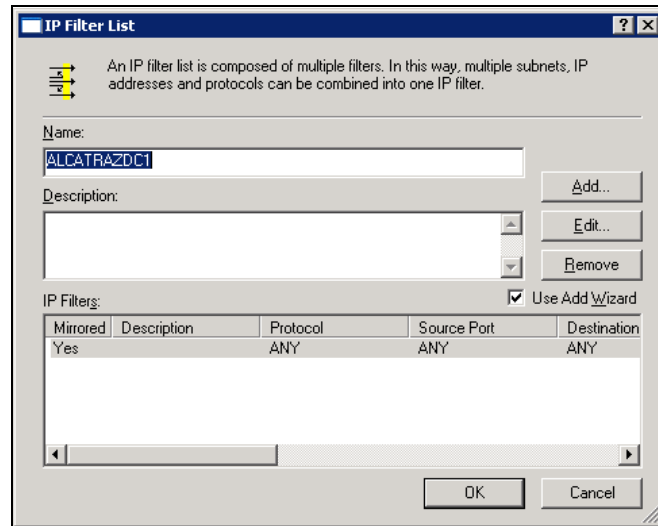
Note that various machines within the Control System environment are configured without authentication or tunnels.

9. Create the the Domain Controller rule. Configuring Rules for this node is critical to avoid locking yourself out of the system.

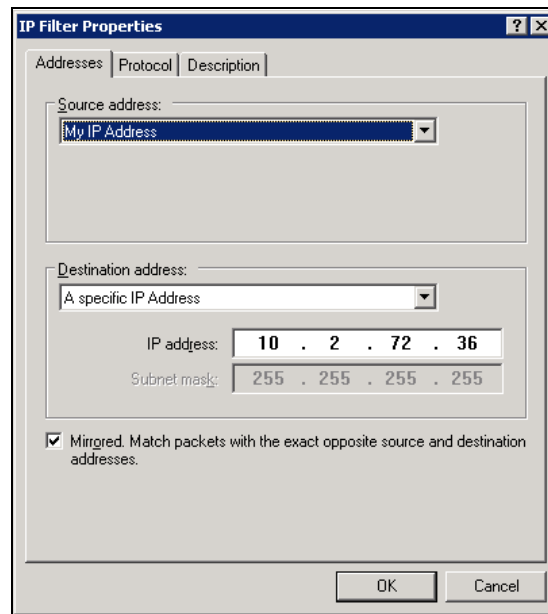
In this example, the **ALCATRAZDC1** rule is configured to permit communication without constraint.



10. Click **Edit**.



11. Click **Edit**.



The Properties for this rule ensure that all packets are matched with the exact source and destination addresses.

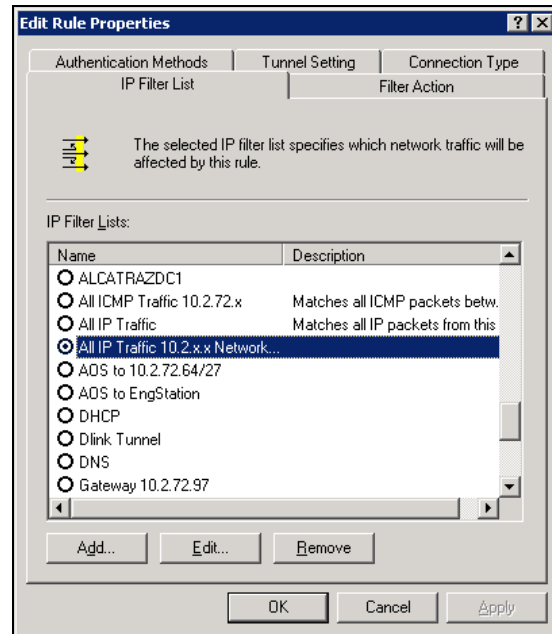
The previous graphic shows the IP address for the domain controller. Repeat these steps for each domain controller.

The **Protocol** and **Description** tabs can be left with the default settings.

To configure the IPSec Security Rule

The following example describes a suggested configuration for the rule that enables IPSec communication.

1. Select the **All IP Traffic** rule.
2. Click **Edit**.

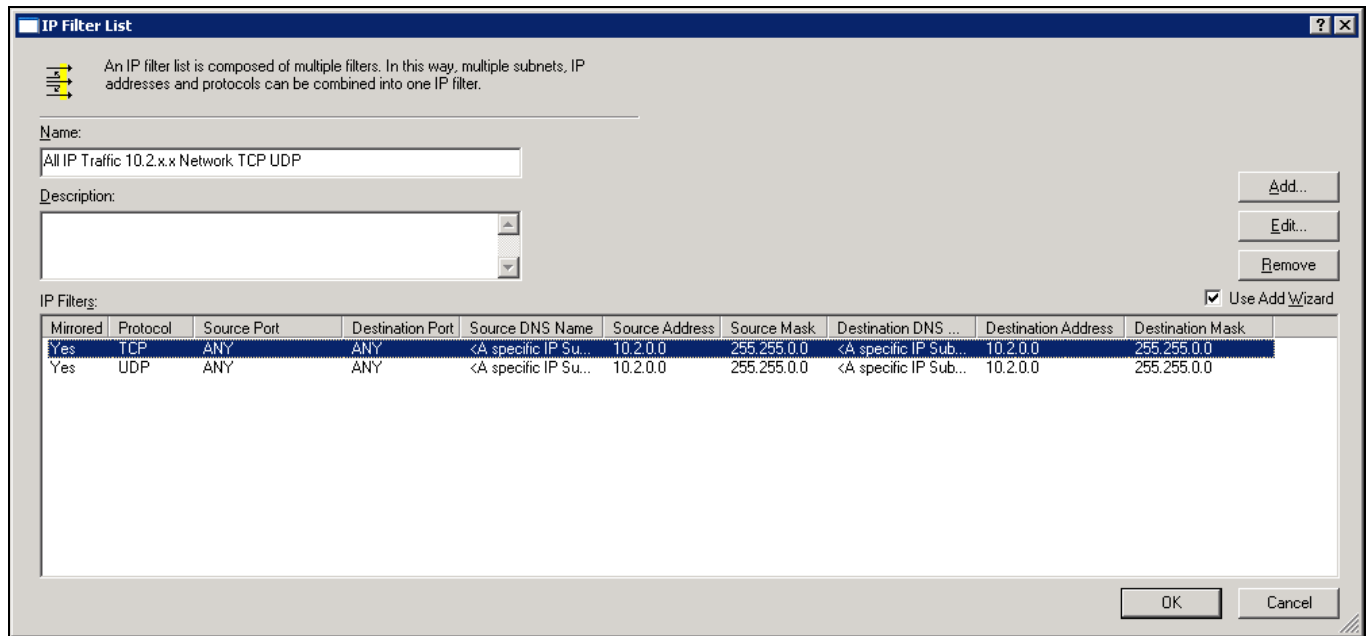


3. Scroll down to the **All IP Traffic** Filter List item. It is the only rule included in this example.

4. Click **Edit**.

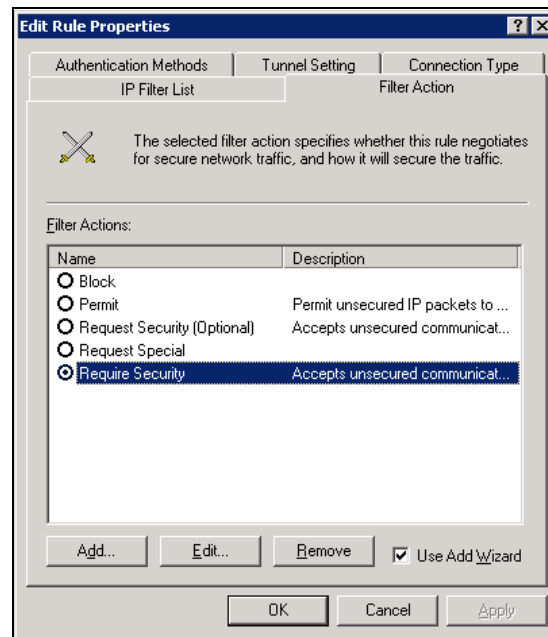
The **IP Filter List** dialog box for this item has been resized for clarity.

Note that two protocols are included, running on the PCN subnet:

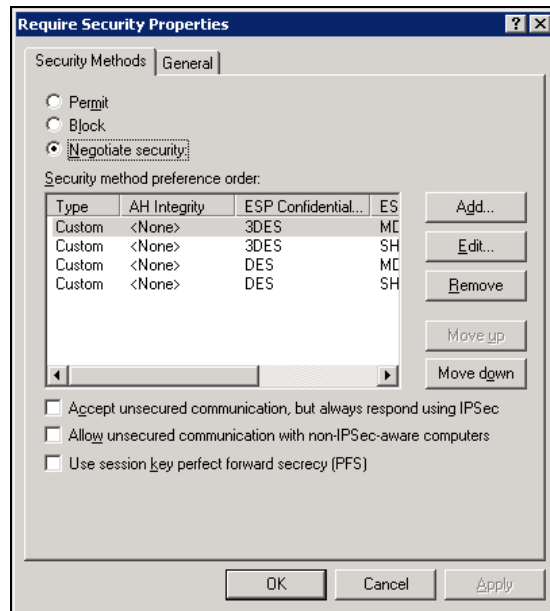


Subnet configuration is performed by editing the item.

5. Click **OK** to save the settings and exit the dialog box.
6. Select the **Filter Action** tab.



7. Select **Require Security** and click **Edit**.



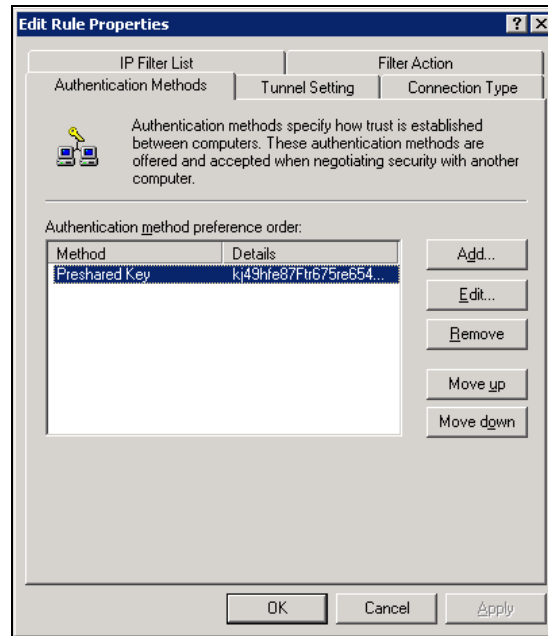
8. Leave the lower options unchecked. The options must be unchecked in order to enforce IPSec.

In this example the **MD5** Rule is moved to the highest priority above its corresponding **SHA1** Rule. Message Digest 5 (MD5) is set as the high priority because it offers the highest available message security.

Note Click [here](#) for more information on MD5 and SHA1 security attributes.

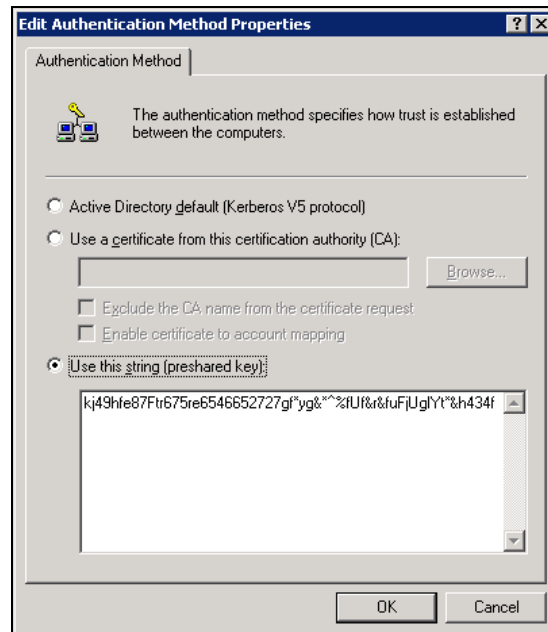
9. Click **OK** to exit this dialog box.

10. Select the **Authentication Methods** tab.



The **Preshared Key** is listed.

11. Click **Edit**.



Active Directory default and certificates can be configured as trusted authentication. This example uses only the existing preshared key.

12. Click **OK**. Other tab configurations are listed below:
 - **Connection Type** = All network connections.
 - **Tunnel Setting** = This rule does not specify an IPSec tunnel.
13. Click **Cancel** to exit the **Edit Rule Properties** dialog box.

To configure the RMC Security Rule

Configure the **RMC** (Redundant Message Channel) to permit all communication for the network (equal to the RMC interface).

The following graphic shows the base IP and Subnet configuration for the RMC:

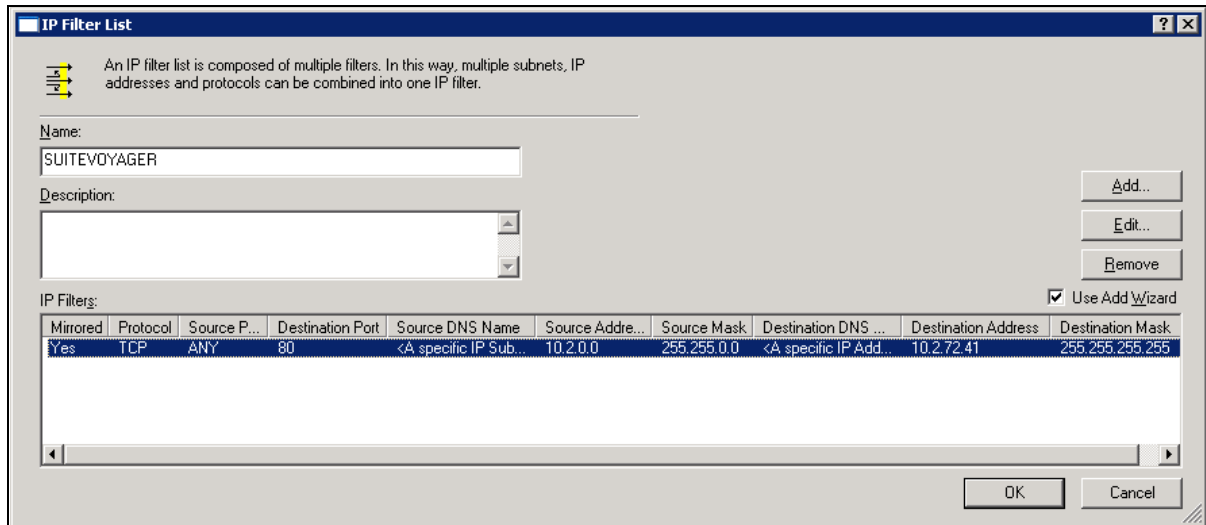
The image shows a Windows-style dialog box titled "IP Filter Properties". It has three tabs: "Addresses", "Protocol", and "Description". The "Addresses" tab is selected. Inside the dialog, there are two main sections: "Source address:" and "Destination address:". Each section has a dropdown menu currently showing "A specific IP Subnet". Below each dropdown are two input fields: "IP Address:" and "Subnet mask:". Both sections have the IP address set to "10 . 27 . 0 . 0" and the subnet mask set to "255 . 255 . 0 . 0". At the bottom of the dialog, there is a checkbox labeled "Mirrored. Match packets with the exact opposite source and destination addresses." which is checked. "OK" and "Cancel" buttons are at the bottom right.

This IP Filter item is important because the RMC is connected as a private network between Redundant Industrial Application Server Nodes, and is not considered vulnerable to external security threats. Adding IPSec to the normal RMC traffic is unnecessary and could negatively affect performance.

To configure the Web Server Security Rule

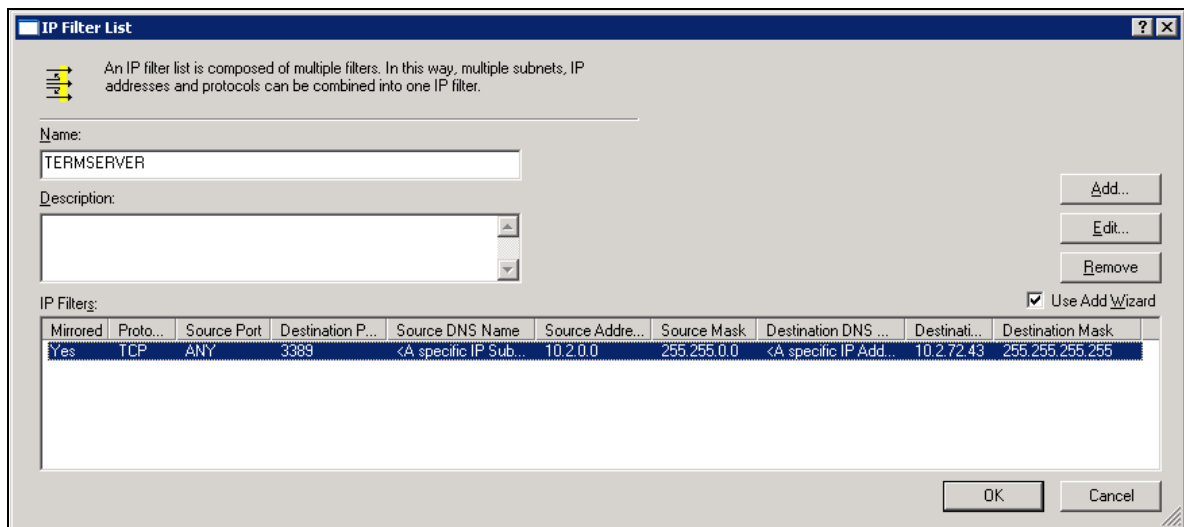
Configure the Web Server node to permit access. In this example, the Web Server node is **SUITEVOYAGER**.

The Filter list editor for the SuiteVoyager Security Rule is shown in the following graphic with the destination **Port 80**:



To configure the Terminal Server Security Rule

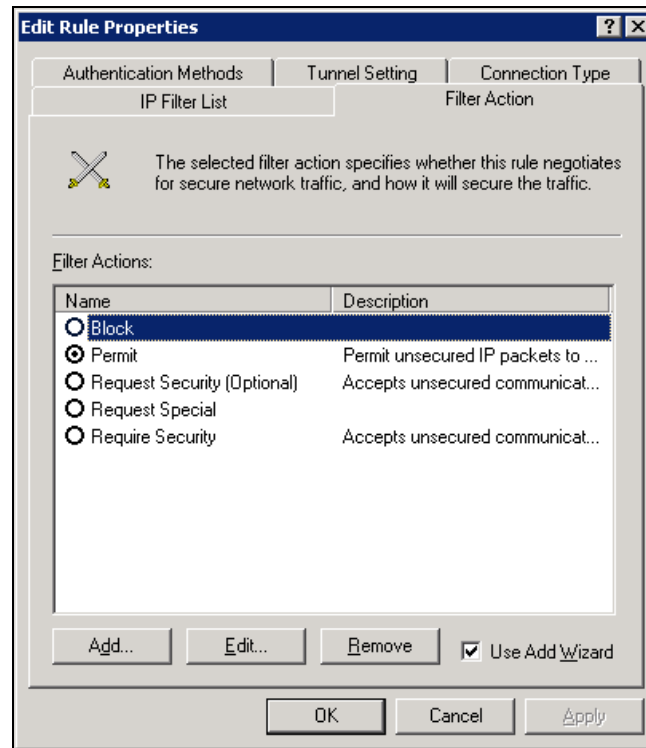
The following graphic shows the properties for the Terminal Server Security Rule. Note the port listing and other properties:



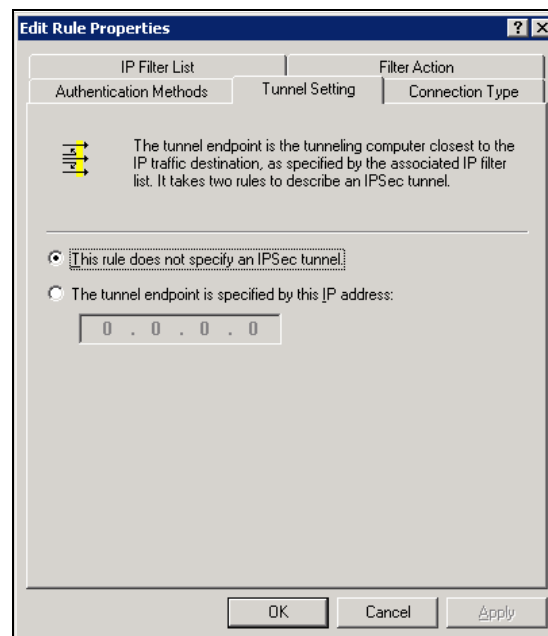
- Click **OK** to exit this dialog box and return to the main **Edit Rule Properties** dialog box.

15. Select the **Filter Action** tab.

In this example, unsecured IP packets are permitted:



16. Select the **Tunnel Setting** tab.



The **This Rule does not specify an IPSec tunnel** option is selected.

Note Tunnel configuration is explained in the following section.

17. Click **OK** or **Cancel** to close all dialog boxes and return to the **Group Policy Object Editor**.

The **Group Policy Object Editor** is the target interface and can be reached from the Active Directory Users and Computers MMC.

Configuration example of Unsecured Device Communication

Unsecured devices include PLCs, VPN devices, etc. IPSec Tunnel Mode is used to provide secure communication between the unsecured device and its endpoint device (a VPN device).

For more detailed information about using IPSec for domain isolation, how it works, and more details about how to configure it, see Appendix A, "References for more help and information," for several links to Microsoft IPSec and domain isolation websites and guidance manuals.

Warning: It is highly recommended that the setup shown within this chapter should be done by an MCSE Security certified Domain Administrator. Personnel who have not had the benefit of this particular training and experience may not understand key concepts of the Active Directory and domain isolation setup. Additionally, if your automation system is being certified or audited, it may not pass if you do not have the properly credentialed personnel establish the IPSec domain isolation security perimeter for the ICS/SCADA System.

Note Construction of the necessary rules and filters for your particular domain isolation setup may be substantially reduced by applying Microsoft Update KB 914841.

<http://www.microsoft.com/downloads/details.aspx?familyid=C44DFDA8-48AE-4868-89A6-67F7612ADFB1&displaylang=en>

Configuring IPSec Tunnel Mode

The following section provides configuration options for an Organizational Unit designed for IPSec communication between unsecured devices.

The Security Rules in this example are:

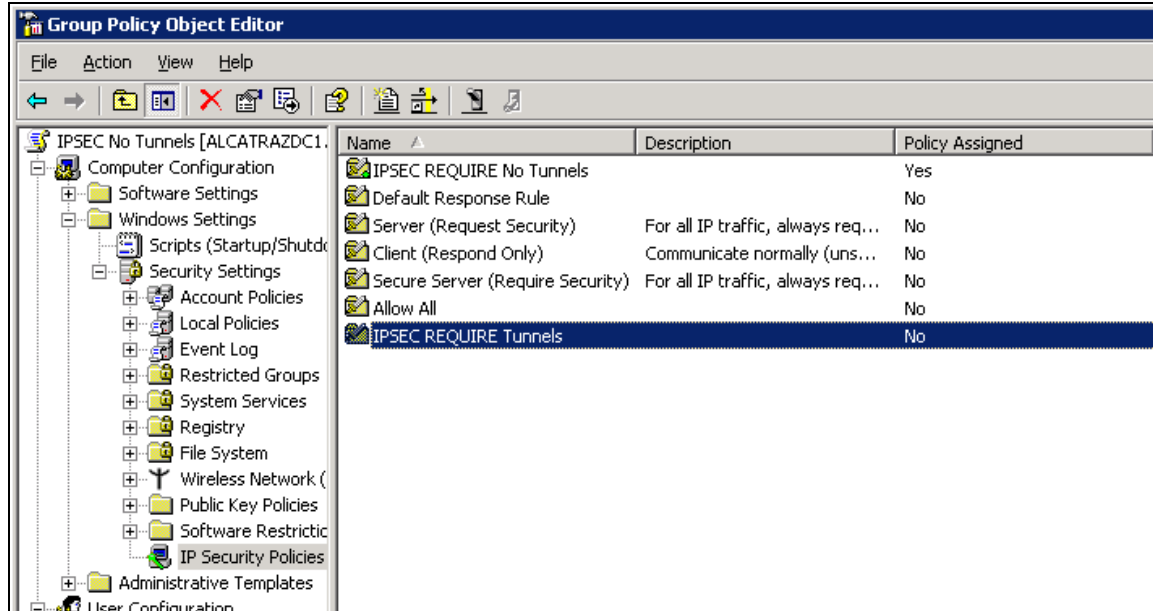
- **1 P1 Tunnel PLC1 to AOS**
- **1 P1 Tunnel AOS to PLC1**

The examples shown in the following graphics describe the pair of Rules configured as VPN endpoints.

To configure IPSEC REQUIRE Tunnels Organizational Unit

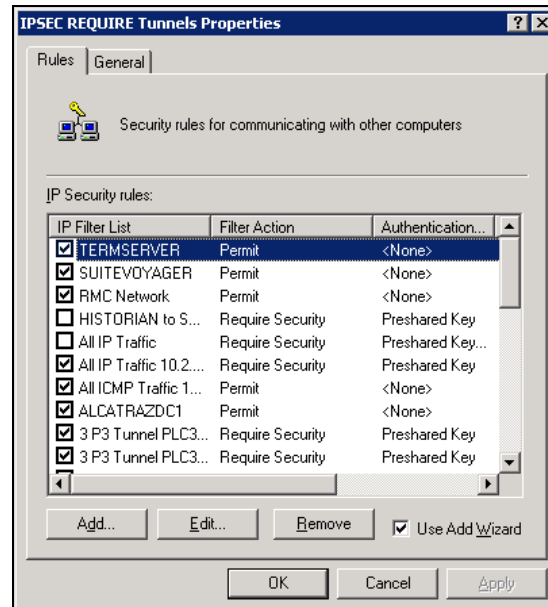
From the **Group Policy Object Editor**:

1. Highlight and right-click the **IPSEC REQUIRE Tunnels** Group Policy object.

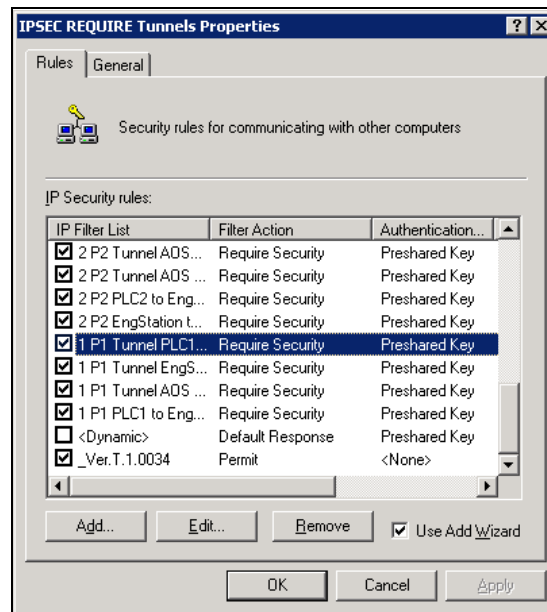


2. Select **Properties**.

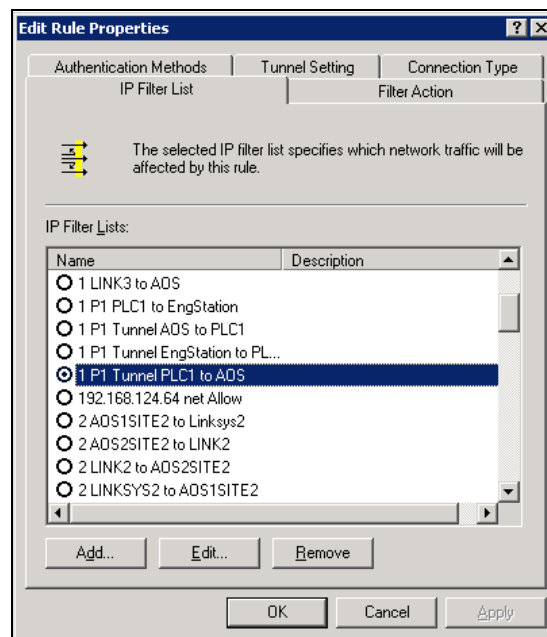
Click the **Add** button to add Security Rules for the VPN Tunnels. The following graphic shows the default highlight at the top of the list (the target example appears further down the list):



3. Scroll down to the **1 P1 Tunnel PLC1 to AOS** Security Rule. Note that the Filter Action requires security and that a Preshared Key exists. If this were a new Security rule, IP Filter lists and other elements would be added at this point.

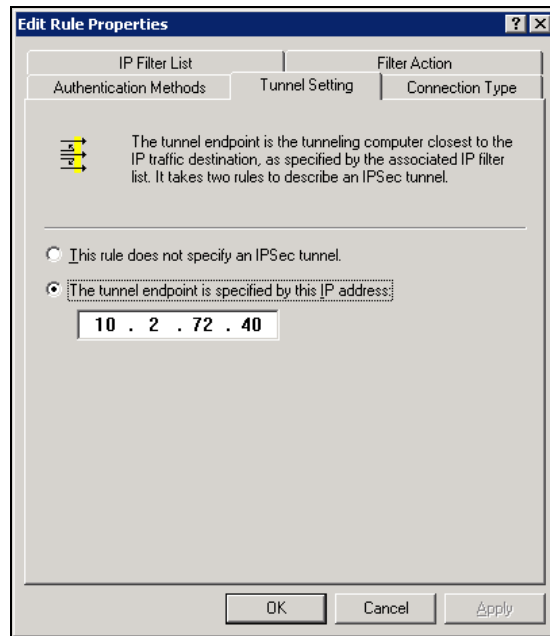


4. Click **Edit**. An IP Filter List item is selected. Its descriptive name (**1P1 Tunnel PLC1 to AOS**) is linked to the previous Security Rule:



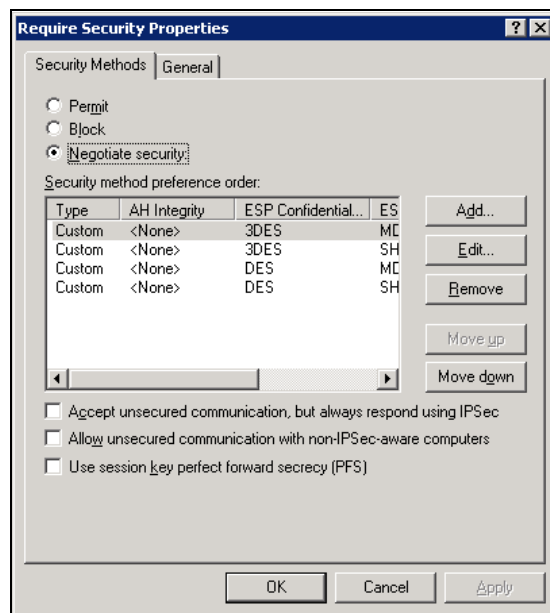
Note Rule Properties are retained and available for re-use by other devices.

5. Select the **Tunnel Setting** tab.



Note the tunnel endpoint setting specified by the IP address (10.2.72.40/AOS node):

6. Click **Cancel** to return to the main **Edit Rule Properties** dialog box.
7. Select the **Filter Action** tab, then highlight the **Require Security** option.
8. Click **Edit**.

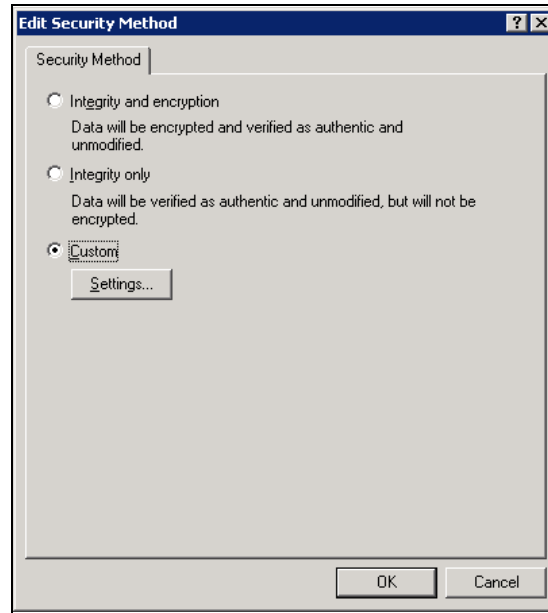


9. Leave the lower options unchecked. The options must be unchecked in order to enforce IPSec.

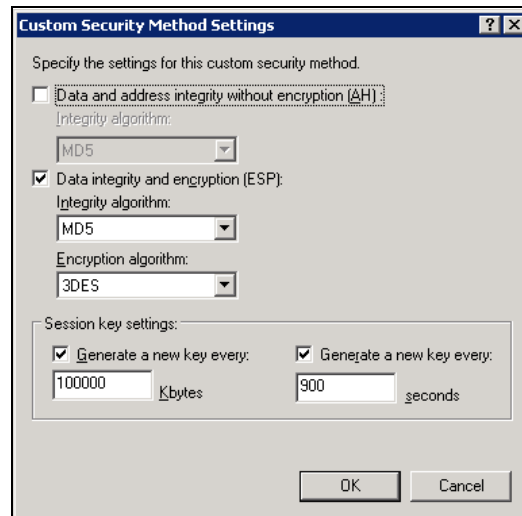
In this example the **MD5** Rule is moved to the highest priority above its corresponding **SHA1** Rule. Message Digest 5 (MD5) is set as the high priority because it offers the highest available message security.

Note Click [here](#) for more information on MD5 and SHA1 security attributes.

10. Select a Security method and click **Edit**.
11. Click the **Settings** button that appears below the **Custom** option:



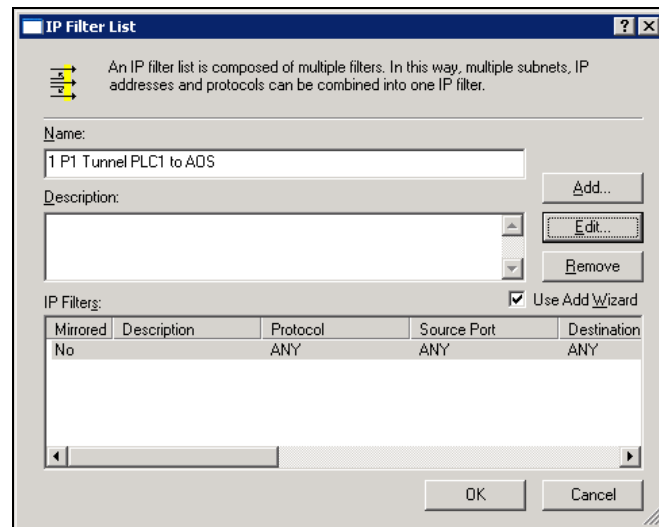
The **Custom Security Method Settings** dialog box appears:



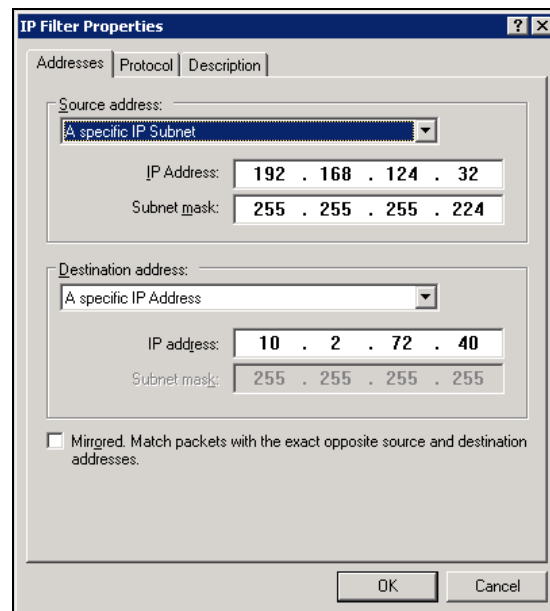
This dialog box enables customized security settings, including Encryption algorithm selection, and generating new keys.

12. Return to the main Edit Rule Properties dialog box by clicking OK to exit other dialog boxes.
13. Select the **IP Filter List** tab.
14. Select the **1P1 Tunnel to PLC1 to AOS** IP Filter list item (scroll down the list).
15. Click **Edit**.

The **IP Filter List** dialog box appears.



16. Click **Edit**.



This dialog box displays the following:

- The **specific IP Subnet**, which is the network behind the VPN endpoint.

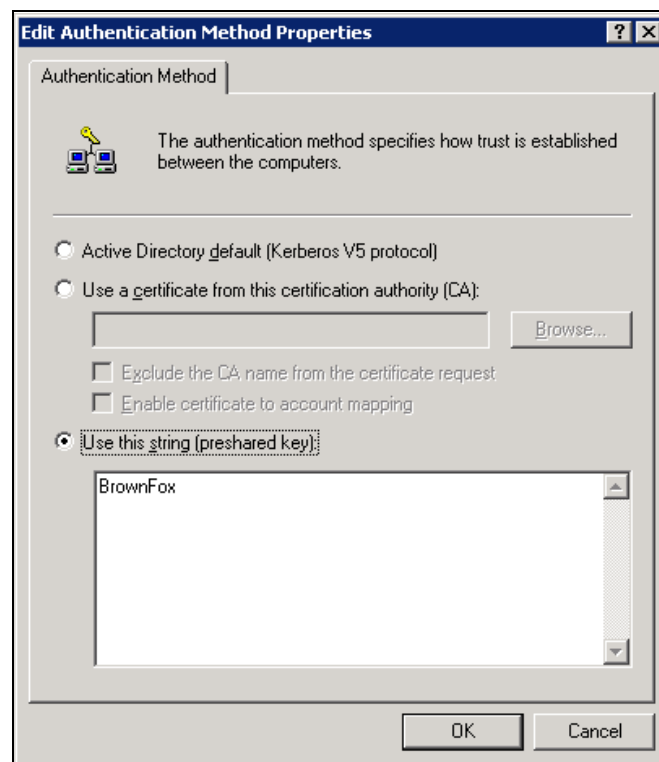
- The **Destination** IP address is the endpoint address shown in the **Tunnel Setting** tab panel (**10.2.72.40/AOS node**).
 - The Filter is *not* mirrored.
17. Configure the specific source and destination address, then click **OK** to exit the **Properties** dialog boxes.

In this example the **Source** IP/Subnet address is **192.168.124.32/255.255.255.224**.

The **Destination** IP address is **10.2.72.40**.

18. Click **OK** until the **Edit Rule Properties (1P1 Tunnel PLC1 to AOS rule)** dialog box appears.
19. Select the **Authentication Methods** tab, then **Edit**.

The following graphic shows a preshared, unique key string:



This string must match the key on the VPN Endpoint device and should be different than the key used in Transport mode. For example:

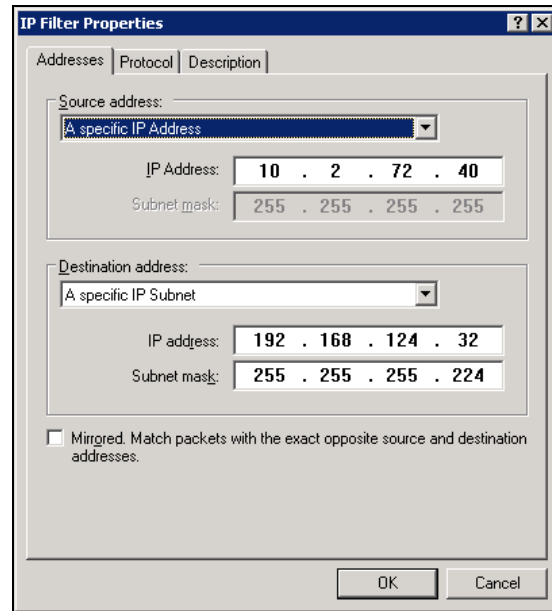
Transport Mode rule	Key 1
VPN Tunnel1 pair of rules	Key 2
VPN Tunnel2 pair of rules	Key 3
VPN Tunnel3 pair of rules	Key 4

20. Click **OK** until the main **Tunnels Properties** list appears.

To configure the VPN Tunnel in the other direction

21. Select the **1 P1 Tunnel AOS to PLC1** Security Rule.
22. Select the **1 P1 Tunnel AOS to PLC1** Rule Property.

Note the Source and Destination IP addresses correspond to the previous settings.



Each tunnel configuration must be configured as a pair as in the previous graphics:

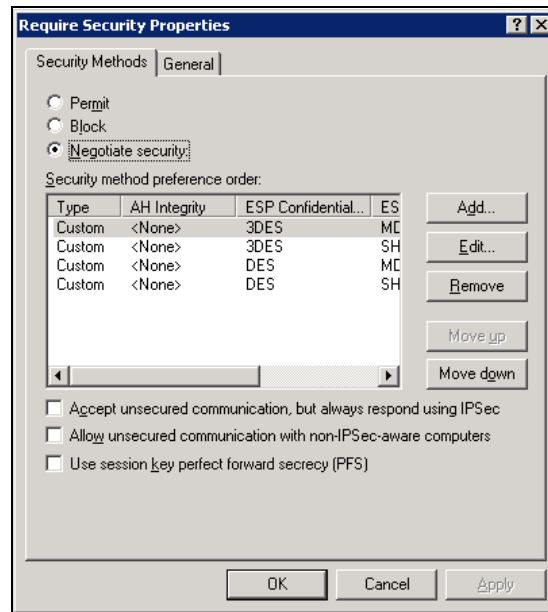
- The **specific IP Address** is the **10.2.72.40/AOS** node.
- The **Destination** IP/Subnet address is the endpoint address shown in the **Tunnel Setting** tab panel (**192.168.124.32/PLC**).
- The Filter is *not* mirrored.

Note Neither IP Address Filter property dialog box is configured for **Mirrored Match** packets.

23. Click **OK**.
24. Select the **Filter Action** tab.

25. Select the **Require Security** item and click **Edit**.

Ensure the **Security Methods** settings for this rule are the same as the paired rule:



26. Click **OK** to exit all Properties configuration dialog boxes.

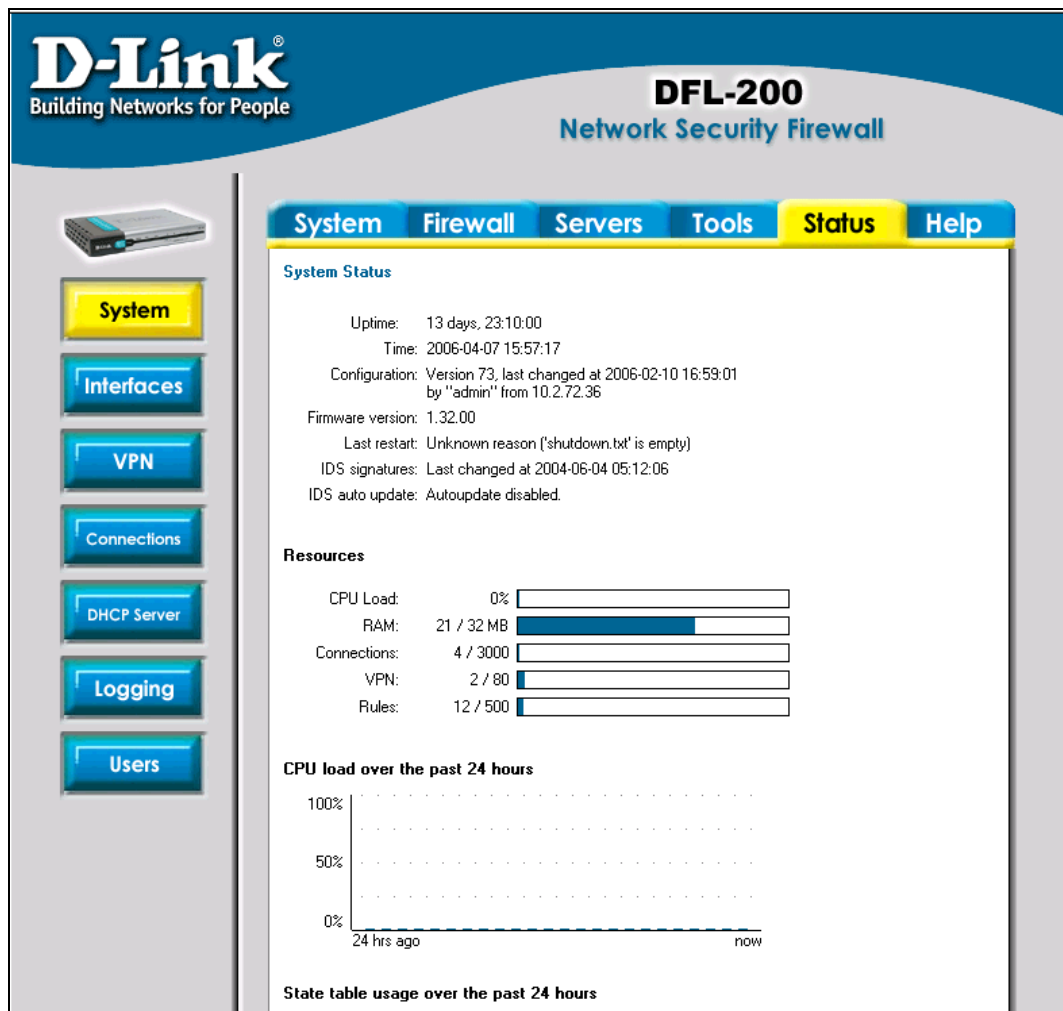
Monitoring the VPN Device

The device used in the following example is D-Link, but most VPN devices have similar VPN configuration settings.

The following example shows the VPN Endpoint Security Rules shown in "To configure IPSEC REQUIRE Tunnels Organizational Unit" on page 224.

Status

Status monitoring returns performance information:



Configuration example of Firewall/VPN Configuration

This example shows two configurations terminating at two nodes. Only the **AOS Tunnel P1** configuration is covered as it matches the window VPN settings shown in previous pages.

D-Link®
Building Networks for People

DFL-200
Network Security Firewall

System **Firewall** Servers Tools Status Help

VPN Tunnels

Pick a VPN tunnel to edit from the below list:

[Help](#)

IPsec Tunnels

Name	Local Net	Remote Net	Remote Gateway	
AOSTunnelP1	192.168.124.32/27	10.2.72.40	10.2.72.40	[Edit]
EngStationPLC1	192.168.124.32/27	10.2.72.44	10.2.72.44	[Edit]

[Add new](#)

L2TP / PPTP Client

Name	Type	Remote Gateway	User	IPsec
Add new PPTP client				
Add new L2TP client				

L2TP / PPTP Server

Name	Type	Outer IP	Inner IP	IPsec
Add new PPTP server				
Add new L2TP server				

Click the **EDIT** link to view the **AOSTunnelP1** configuration.

Firewall/VPN Configuration/AOSTunnelP1

This pre-shared key is different from the Tunnel Mode pre-shared key. The following graphic shows the key setting and the Pre-shared key entry. The Pre-shared key entry must match the corresponding rule in the Windows IPSec configuration.

Note The following graphics represent the same **VPN/Firewall** tab pane.

The screenshot displays the D-Link DFL-200 Network Security Firewall configuration web interface. The top navigation bar includes tabs for System, Firewall (selected), Servers, Tools, Status, and Help. On the left sidebar, there are buttons for Policy, Port Mapping, Users, Schedules, Services, VPN (highlighted in yellow), Certificates, and Content Filtering. The main content area is titled 'VPN Tunnels' and shows the configuration for 'AOSTunnelP1'. The 'Name' field is set to 'AOSTunnelP1' and the 'Local Net' is '192.168.124.32/27'. Under the 'Authentication' section, the 'PSK - Pre-Shared Key' option is selected. The 'PSK' and 'Retype PSK' fields are masked with asterisks. The 'Certificate-based' option is unselected. The 'Local Identity' dropdown shows 'Admin - CN=0013469C3DEC'. The 'Certificates' list is empty, with a note: 'Use ctrl/shift click to select multiple certificates. To use ID lists below, you must select a CA certificate.' The 'Identity List' dropdown shows '[no list]'. At the bottom, the 'Tunnel type' section has the 'Roaming Users - single-host IPsec clients' option selected.

D-Link®
Building Networks for People

DFL-200
Network Security Firewall

System **Firewall** Servers Tools Status Help

VPN Tunnels

Edit IPsec tunnel **AOSTunnelP1**:

Name: AOSTunnelP1
Local Net: 192.168.124.32/27

Authentication:

☒ **PSK - Pre-Shared Key**

PSK:
Retype PSK:

☐ **Certificate-based**

Local Identity: Admin - CN=0013469C3DEC
Certificates:

Use ctrl/shift click to select multiple certificates.
To use ID lists below, you must select a CA certificate.

Identity List: [no list]

Tunnel type:

☒ **Roaming Users - single-host IPsec clients**

The following figure shows the AOS node IP address in the **LAN-to-LAN** tunnel field:

Tunnel type:

☐ **Roaming Users** - single-host IPsec clients

IKE XAuth: ☐ Require user authentication via IKE XAuth to open tunnel.

☒ **LAN-to-LAN tunnel**

Remote Net:

Remote Gateway:

The gateway can be a numerical IP address, DNS name, or range of IP addresses for roaming / NATed gateways.

Route: ☒ Automatically add a route for the remote network.

Proxy ARP: ☐ Publish remote network on all interfaces via Proxy ARP.

IKE XAuth client: ☐ Pass username and password to peer via IKE XAuth, if the remote gateway requires it.

XAuth Username:

XAuth Password:

☐ Delete this VPN tunnel

Advanced Apply Cancel Help

The following figure shows the bottom of the **VPN/Firewall** tab panel:

IPsec Tunnels

Name	Local Net	Remote Net	Remote Gateway	
AOSTunnelP1	192.168.124.32/27	10.2.72.40	10.2.72.40	[Edit]
EngStationPLC1	192.168.124.32/27	10.2.72.44	10.2.72.44	[Edit]

[Add new](#)

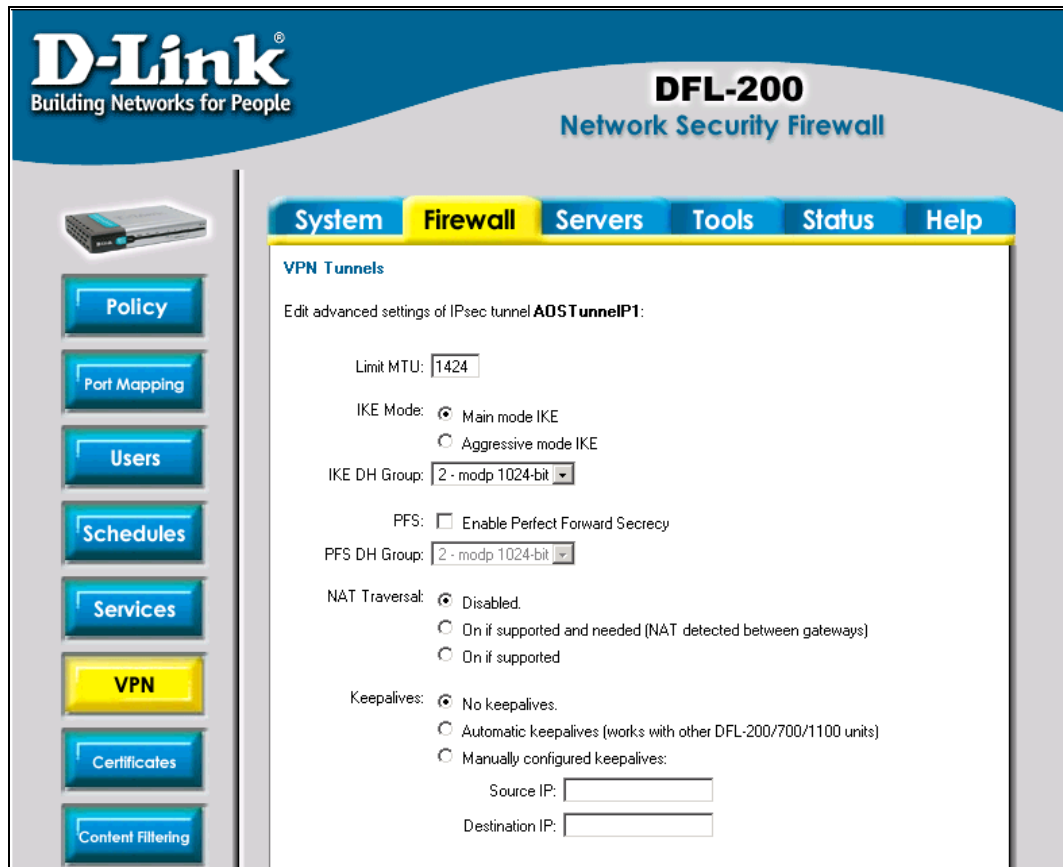
L2TP / PPTP Client

Name	Type	Remote Gateway	User	IPsec
Add new PPTP client				
Add new L2TP client				

L2TP / PPTP Server

Name	Type	Outer IP	Inner IP	IPsec
Add new PPTP server				
Add new L2TP server				

Click the **Advanced** link. Configuration options include IKE Proposal configuration, Keepalives, etc.



The screenshot displays the web interface of a D-Link DFL-200 Network Security Firewall. The top header features the D-Link logo and the model name. A navigation bar includes tabs for System, Firewall, Servers, Tools, Status, and Help. A left sidebar contains buttons for Policy, Port Mapping, Users, Schedules, Services, VPN (highlighted), Certificates, and Content Filtering. The main content area is titled 'VPN Tunnels' and shows the configuration for 'A0STunnelP1'. The settings include:

- Limit MTU: 1424
- IKE Mode: ☒ Main mode IKE, ☐ Aggressive mode IKE
- IKE DH Group: 2 - modp 1024-bit
- PFS: ☐ Enable Perfect Forward Secrecy
- PFS DH Group: 2 - modp 1024-bit
- NAT Traversal: ☒ Disabled, ☐ On if supported and needed (NAT detected between gateways), ☐ On if supported
- Keepalives: ☒ No keepalives, ☐ Automatic keepalives (works with other DFL-200/700/1100 units), ☐ Manually configured keepalives (with Source IP and Destination IP input fields)




Note the **Life KB** and **Life Sec** fields. These values should match the Windows-based settings.

Likewise, move **SHA-1** above **MD5** to conserve CPU (as shown in the following graphic):

IKE Proposal List				
	Cipher	Hash	Life KB	Life Sec
#1:	AES-128 Allowed:128-256	SHA-1	0	28800
#2:	AES-128 Allowed:128-256	MD5	0	28800
#3:	3DES	SHA-1	0	28800
#4:	3DES	MD5	0	28800
#5:	DES	SHA-1	0	28800
#6:	DES	MD5	0	28800
#7:	-	MD5	0	0
#8:	-	MD5	0	0

IPsec Proposal List				
	Cipher	HMAC	Life KB	Life Sec
#1:	AES-128 Allowed:128-256	SHA-1	0	3600
#2:	AES-128 Allowed:128-256	MD5	0	3600
#3:	3DES	MD5	10000	900
#4:	3DES	SHA-1	10000	900
#5:	DES	MD5	10000	900
#6:	DES	SHA-1	10000	900
#7:	-	MD5	0	0
#8:	-	MD5	0	0

"AES-128 Allowed:128-256" means that this unit will propose 128 bit encryption to the remote end when establishing an outbound tunnel, and will accept any cipher key sizes between 128 and 256 (inclusive) when receiving inbound tunnels.




Apply Cancel Help

Configure the firewall to block all non-IPSec traffic in both directions and be sure no NAT (Network Address Translation) is utilized (as shown in the following graphic):

D-Link®
Building Networks for People

DFL-200
Network Security Firewall

System Firewall Servers Tools Status Help

Firewall Policy

Show policy: [LAN->WAN](#) [LAN->DMZ](#) [WAN->DMZ](#)
[WAN->LAN](#) [DMZ->LAN](#) [DMZ->WAN](#)

Show custom policy: LAN -> WAN Show

Settings for LAN->WAN policy:

NAT: ☐ Hide source addresses (many-to-one NAT)
☒ No NAT - requires public IP addresses on LAN network.

Apply Cancel Help

Select "Add New" below, or select a rule from the list to edit it:

LAN->WAN Policy

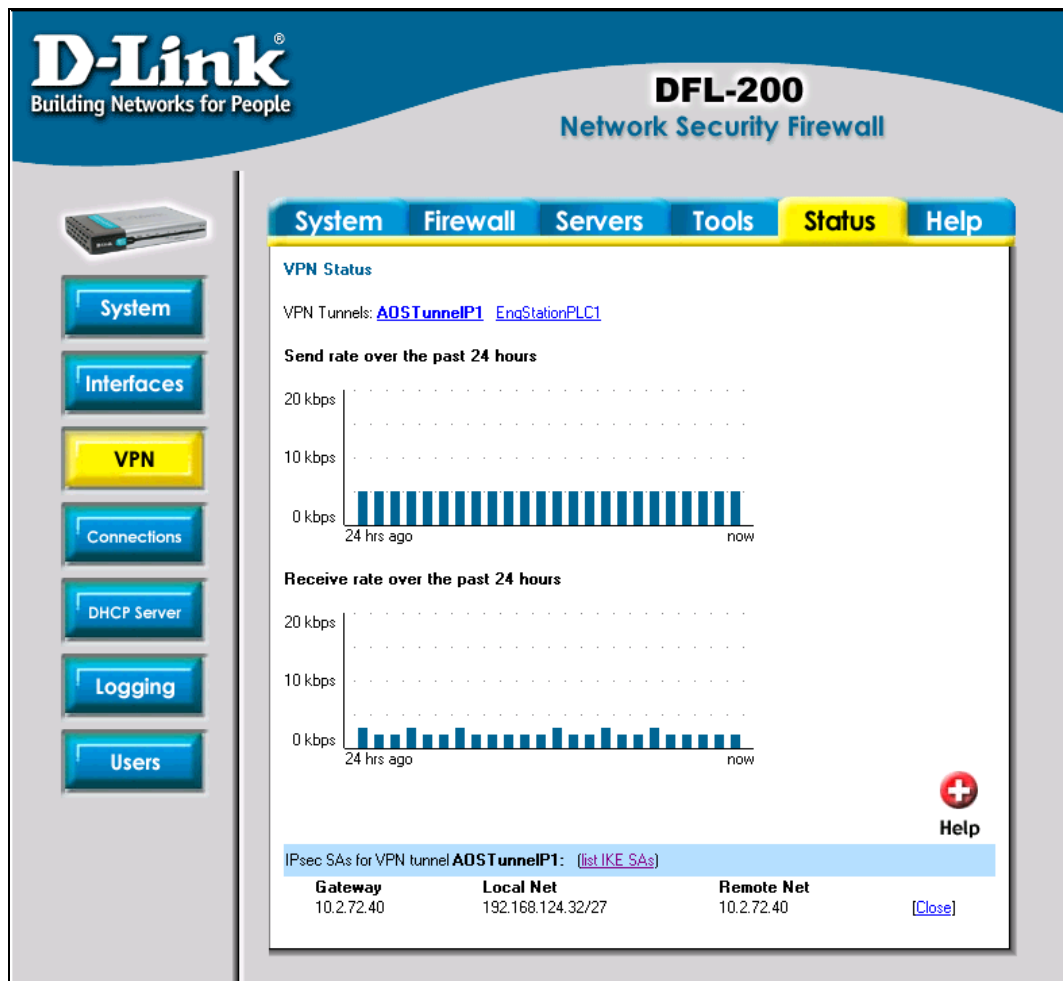
Name	Action	Source	Destination	Service	Move
#1 allow_ipsec	Allow	Any	Any	ipsec-suite	↓ [Edit]
#2 deny_all	Drop	Any	Any	All Protocols	↑ ↓ [Edit]
#3 allow_standard	Allow	Any	Any	All Protocols	↑ [Edit]

[\[Add new\]](#)

Order of evaluation ↓

If no rule matches, the connection will be denied and logged.

The following graphic displays the negotiated SA (Security Association timeout values) at the bottom of the screen, and indicates the traffic history over the VPN:



System/Routing Configuration

Routing information is displayed in the following graphic:

The screenshot shows the D-Link DFL-200 Network Security Firewall web interface. The left sidebar contains navigation buttons: Administration, Interfaces, Routing (highlighted), Logging, and Time. The main content area has tabs for System, Firewall, Servers, Tools, Status, and Help. The 'Routing Table' section is active, displaying a table of routes and an 'Add new' link.

D-Link®
Building Networks for People

DFL-200
Network Security Firewall

System | Firewall | Servers | Tools | Status | Help

Routing Table

Pick a route to edit from the below list:

Note that routing table ordering does not matter; smaller routes are always picked above larger ones.

[Help](#)

Interface	Network	Gateway	Additional IP	Proxy ARP
LAN	192.168.124.32/27			[Edit]
WAN	10.2.72.32/27			[Edit]
WAN	0.0.0.0/0	10.2.72.33		[Edit]
DMZ	127.0.0.0/24			[Edit]
ADSTunnelIP1	10.2.72.40			Auto
EngStationPLC1	10.2.72.44			Auto

[\[Add new\]](#)

System/Interface/LAN

The following graphic shows the LAN interface per our lab graphics:

The screenshot shows the D-Link DFL-200 Network Security Firewall web interface. The left sidebar contains navigation buttons: Administration, Interfaces (highlighted), Routing, Logging, and Time. The main content area has tabs for System, Firewall, Servers, Tools, Status, and Help. The 'Interface Settings' section is active, displaying the configuration for the LAN interface.

D-Link®
Building Networks for People

DFL-200
Network Security Firewall

System | Firewall | Servers | Tools | Status | Help

Interface Settings

Edit settings of the **LAN** interface:

IP Address:

Subnet Mask: - 32 hosts (/27)

[Apply](#) [Cancel](#) [Help](#)

Available interfaces

LAN	[Edit]
WAN (Static)	[Edit]
DMZ	[Edit]

IPSec Configuration Summary

- The previous examples are derived from a lab environment and designed to show the basic steps necessary to create and administer the IPSec Organizational Units and their appropriate security rules.
- No "upper boundary" data is available.
- The examples are designed to familiarize the user with the the Windows-standard interfaces used to perform IPSec administration.
- IPSec between machines (within the Control System) is configured without extra Security Rules (Transport mode - **REQUIRE No Tunnels**).
- IPSec between the AOS node and the unsecured device is accomplished by configuring two "tunnels" or VPN end-points, one to send, and one to receive data.

IPSec Configuration Best Practices

- Use separate OUs in the Active Directory to provide a user-friendly interface and make configuration more efficient.
- Use a recognized naming convention for the OUs.
- Cascade the OU naming convention to the related security rules and properties.
- It is possible to have one VPN Endpoint proxy for multiple PLC devices if they are in the same location.

A P P E N D I X A

References for more help and information

This Appendix lists several References you can consult for more information.

Contents

- Organizations
- Microsoft Domain Isolation
- Articles and Books
- Useful RSS Feeds
- Additional Links

Organizations:

- **Wonderware Technical Support**, <http://www.wonderware.com>, 1-800-WONDER-1, Customer Service Subscriptions, Application and ICS Security Consultation Services.
- **NIST** (National Institute for Standards and Technology)
<http://csrc.nist.gov>
- **PCSF** (Process Control Systems Forum) <http://www.pcsforum.org>
- **US-CERT** (United States Computer Emergency Readiness Team)
<http://www.us-cert.gov/>
- **ISA** (The Instrumentation, Automation and Systems Society)
<http://www.isa.org>
- **NERC** (North American Electric Reliability Council)
<http://www.nerc.com/>
- **AGA** (American Gas Association) <http://www.aga.org/>
- **API** (American Petroleum Institute) <http://www.api.org/>
- **IEC** (International Engineering Consortium) <http://www.iec.org/>
- **IEEE** (Institute of Electrical and Electronics Engineers, Inc.)
<http://www.ieee.org/portal/site>
- **ISO** (International Organization for Standardization)
<http://www.iso.org/iso/en/ISOOnline.frontpage>

Microsoft Domain Isolation:

- Server and Domain Isolation Using IPsec and Group Policy
(<http://www.microsoft.com/downloads/details.aspx?FamilyId=404FB62F-7CF7-48B5-A820-B881F63BC005&displaylang=en>)
- Improving Security with Domain Isolation
(<http://www.microsoft.com/technet/itsolutions/msit/security/ipsecdoisolwp.aspx>)
- Introduction to Server and Domain Isolation with Microsoft Windows
(<http://www.microsoft.com/downloads/details.aspx?FamilyID=9a3e2b2b-695d-4ff9-bcb1-5f2f3001845e&DisplayLang=en>)
- Server Isolation with Microsoft Windows Explained
(<http://www.microsoft.com/downloads/details.aspx?FamilyID=93bed81a-d073-4c2e-866f-e062dc2213b7&DisplayLang=en>)
- Windows Server 2003 IPsec Website
(<http://www.microsoft.com/technet/itsolutions/network/ipsec/default.aspx>)
- TechNet Support WebCast: How to use IPsec to help secure network traffic (<http://support.microsoft.com/default.aspx?kbid=888266>)
- Using IPsec for Network Protection: Part 1 of 2
(<http://www.microsoft.com/technet/community/columns/secmgmt/sm121504.aspx>)

- Using IPSec for Network Protection. Part 2 of 2
(<http://www.microsoft.com/technet/community/columns/secmgmt/sm0105.mspx>)
- How to simplify the creation and maintenance of Internet Protocol (IPSec) security filters in Windows Server 2003 and Windows XP
(<http://support.microsoft.com/default.aspx/kb/914841/en-us>)
- Update for Windows Server 2003 (KB914841) [Filter Reduction Patch]
(<http://www.microsoft.com/downloads/details.aspx?familyid=C44DFDA8-48AE-4868-89A6-67F7612ADFB1&displaylang=en>)

Articles and Books:

- CSB (Chemical Safety Board) <http://www.csb.gov/> 2005 Explosion at BP Refinery, Texas City, Texas
- “IT Survival Guide”, Second Edition, TechRepublic, <http://productorders.techrepublic.com>
- “Rootkits - Subverting the Windows Kernel”, Greg Hoglund & James Butler, ISBN 0-321-29431-9, Addison-Wesley, Pearson Education
- “Windows Forensics and Incident Recovery”, Harlan Carvey, ISBN 0-321-20098-5, Addison-Wesley, Pearson Education
- “Administrator’s Guide to Active Directory”, Second Edition, TechRepublic, <http://productorders.techrepublic.com>
- “Administrator’s Guide to TCP/IP”, Second Edition, TechRepublic, <http://productorders.techrepublic.com>

Useful RSS Feeds

- <http://www.wonderware.com/support/mmi/RSS/feeds/WWSecurityCentralFeed.xml>
- <http://feeds.feedburner.com/techtargget/searchsecurity/networksecurity>
- <http://feeds.feedburner.com/techtargget/Searchsecurity/SecurityWire>
- <http://feeds.feedburner.com/techtargget/searchsecurity/networksecurity>
- http://news.zdnet.com/2509-1_22-0-20.xml

Additional Links

- American Gas Association Report 12: Cryptographic Protection of SCADA Communications Part 1: Background, Policies and Test Plan:
http://www.gtiservices.org/security/AGA12_part1_draft6.pdf
- ANSI/ISA-TR99.00.02-2004: Integrating Electronic Security into the Manufacturing and Control Systems Environment:
<http://www.isa.org/Template.cfm?Section=Standards1&template=/Ecommerce/ProductDisplay.cfm&ProductID=7380>

- Federal Information Security Management Act (FISMA):
<http://csrc.nist.gov/policies/FISMA-final.pdf>
- FIPS Publication 199: Standards for Security Categorization of Federal Information and Information Systems:
<http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>
- FIPS Publication 200: Minimum Security Requirements for Federal Information and Information Systems:
<http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf>
- FISMA Implementation Project: <http://csrc.nist.gov/sec-cert/>
- IAONA: <http://www.iaona.org/home/downloads.php>
- Insider Threat Study: http://www.cert.org/insider_threat/insidercross.html
- Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector: <http://www.cert.org/archive/pdf/bankfin040820.pdf>
- Integrity checker Tools: <http://integrit.sourceforge.net/>,
<http://www.tripwire.com/>
- ISA-TR99.00.02-2004: Integrating Electronic Security into the Manufacturing and Control Systems Environment:
<http://www.isa.org/Template.cfm?Section=Standards1&template=/Ecommerce/ProductDisplay.cfm&ProductID=7380>
- MD5 <http://www.fastsum.com/>
- Microsoft Technical White Paper: Improving Security with Domain Isolation:
<http://www.microsoft.com/technet/itshowcase/content/ipsecdomisolwp.aspx>
- National Institute of Standards and Technology (NIST)
<http://www.nist.gov/>
- NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks: <http://www.niscc.gov.uk/niscc/docs/re-20050223-00157.pdf>
- NIST Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook: <http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>
- NIST Special Publication 800-18, Rev 1: Guide for Developing Security Plans for Information Systems:
<http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf>
- NIST Special Publication 800-23: Guidelines to Federal Organizations on Security Assurance and Acquisition / Use of Tested / Evaluated Reports:
<http://csrc.nist.gov/publications/nistpubs/800-23/sp800-23.pdf>
- NIST Special Publication 800-26, Rev 1: Assessment Guide for Information Systems and Security Programs:
<http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf>
- NIST Special Publication 800-27 Rev A: Engineering Principles for Information Technology Security (A Baseline for Achieving Security):
<http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf>

- NIST Special Publication 800-28: Guidelines on Active Content and Mobile Code: <http://csrc.nist.gov/publications/nistpubs/800-28/sp800-28.pdf>
- NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems: <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>
- NIST Special Publication 800-31: Intrusion Detection Systems: <http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf>
- NIST Special Publication 800-34: Contingency Planning Guide for Information Technology Systems: <http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf>
- NIST Special Publication 800-35: Guide to Information Technology Security Services: <http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf>
- NIST Special Publication 800-36: Guide to Selecting Information Technology Security Products: <http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf>
- NIST Special Publication 800-37: Guide for the Security Certification and Accreditation of Federal Information Systems: <http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf>
- NIST Special Publication 800-40: Creating a Patch and Vulnerability Management Program: <http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf>
- NIST Special Publication 800-41: Guidelines on Firewalls and Firewall Policy: <http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf>
- NIST Special Publication 800-42: Guideline on Network Security Testing: <http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf>
- NIST Special Publication 800-48: Wireless Network Security: http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf
- NIST Special Publication 800-50: Guide for Mapping Types of Information and Information Systems to Security Categories: <http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V1-final.pdf>
- NIST Special Publication 800-53: Recommended Security Controls for Federal Information Systems: <http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf>
- NIST Special Publication 800-53A: Guide for Assessing Security Controls in Federal Information Systems: <http://csrc.nist.gov/publications/drafts/SP800-53A-spd.pdf>
- NIST Special Publication 800-56: Recommendation on Key Establishment Schemes: <http://csrc.nist.gov/CryptoToolkit/kms/keyschemes-Jan03.pdf>
- NIST Special Publication 800-57: Recommendation for Key Management - Part 1: General: <http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part1.pdf>

- NIST Special Publication 800-58: Security Considerations for Voice Over IP Systems: <http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf>
- NIST Special Publication 800-59: Guideline for Identifying an Information System as a National Security System: <http://csrc.nist.gov/publications/nistpubs/800-59/SP800-59.pdf>
- NIST Special Publication 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories: <http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V1-final.pdf>
- NIST Special Publication 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories: <http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V1-final.pdf>
- NIST Special Publication 800-61: Computer Security Incident Handling Guide: <http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf>
- NIST Special Publication 800-63: Electronic Authentication Guideline: http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf
- NIST Special Publication 800-64: Security Considerations in the Information System Development Life Cycle: <http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf>
- NIST Special Publication 800-65: Integrating IT Security into the Capital Planning and Investment Control Process: <http://csrc.nist.gov/publications/nistpubs/800-65/SP-800-65-Final.pdf>
- NIST Special Publication 800-68, Guidance for Security Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist: <http://csrc.nist.gov/itsec/SP800-68-20051102.pdf>
- NIST Special Publication 800-70: The NIST Security Configuration Checklists Program: http://csrc.nist.gov/checklists/docs/SP_800-70_20050526.pdf
- NIST Special Publication 800-70: Security Configuration Checklists Program for IT Products - Guidance for Checklists Users and Developers: http://csrc.nist.gov/checklists/docs/SP_800-70_20050526.pdf
- NIST Special Publication 800-73: Interfaces for Personal History Verification: <http://csrc.nist.gov/publications/nistpubs/800-73-1/sp800-73-1v7-April20-2006.pdf>
- NIST Special Publication 800-76: Biometric Data Specification for Personal Identity Verification: http://csrc.nist.gov/publications/drafts/800-76-1/SP800-76-1_012407.pdf
- NIST: System Protection Profile: Industrial Control Systems: <http://www.isd.mel.nist.gov/projects/processcontrol/SPP-ICSv1.0.pdf>
- Organization's Critical Assets <http://www.cert.org/octave/>
- Sandia National Laboratories (SNL): <http://www.sandia.gov/>
- Sarbanes Oxley Act: <http://www.sec.gov/about/laws.shtml>
- SHA1 http://www.w3.org/PICS/DSig/SHA1_1_0.html

- Vulnerability Testing of Industrial Network Devices:
<http://www.scadasec.net/oldio/papers/franz-isa-device-testing-oct03.pdf>

Index

A

access
 assess security 40
 assessing security 40
 control 138–139
 physical 120–122
 remote 86–87, 140
 system domain 46
 user access, high-level, risks with 82–83
activities to manage risk, see managing risks
additional security information and resources 19–20, 244–??
anti-virus tools 127, 154
 see also malware
 use with Wonderware software 155
assess vulnerabilities 104–106
attack
 insider 72
 response, see Incident Response
 results 99
attack scenarios 67–68
 see also case studies
audience, book 18
audit
 online activity 81
 system controls adequacy 141–142
 user accounts 80
authentication methods, user 133–137

B

backup and recovery 93–94
 see also contingency planning 93
breach, see attack scenarios, attacks

C

case studies, attacks 70–71
 insider 78–79
 malicious code 85–86
 online activity 81–82
 remote access 87–88
 suspicious employee behavior 89
 terminated employees 91
 user access 84
CERT (US Computer Emergency Readiness Team) 116
certification of Security Controls 118
code, malicious 84–85, 127
communication
 outbound traffic 174–175
 protocols 28
components
 ICS operation 23
 network 25
connections
 increased 40
 insecure 41
 rogue 41
contingency planning 123

control room 122
controls for attack prevention 112, 132
CSSC (Control Systems Security Center) 116
cyber-security team 102–103

D

DCS (Distributed Control Systems) 21
detection, intruder 153
DMZ (Demilitarized Zone) 166

E

employee training 75–76, 107, 119, 132
encryption 143–144, 152
endpoint device 163–164, 200

F

firewall 152–153, 167–173
 issues 179–181
 rules for specific services 176–179
FISMA (Federal Information Security Management Act) 108

H

help, see technical support
hiring policies 120

I

IAONA (Industrial Automation Open Networking Association) 176
ICS (Industrial Control System) 21, 23
impact, security breach 110, 115
incident response planning guidelines 131
industry types
 oil and gas 32
 power 32
 wastewater 32
 water supply 32
insider attacks 72
 see also hiring policies and training, employee
installation steps 196
intruder detection 153
investigation data 92
IPSec
 benefits 189
 configuring 190–193
 organizational unit 210
 transport configuration 211–223
 tunnel configuration 198, 223–240
IPSec (Internet Protocol Security) 188
IT policies 43, 103
IT versus ICS security 183
IT versus ICS security environment 161–163

L

layers of security 194–195

- level 1 195–201
- level 2 205
- level 3 206
- level 4 206–207
- legacy nodes 202–203

M

- malicious code 84–85, 127
- malware 151–154
 - detection software 154
- management involvement 100–101, 102, 132
- managing risks 108–112
- manufacturing
 - batch 22
 - continuous 22
 - process-based 22
- mitigation costs of security risks 107
- multi-homing 94

N

- network 55–59
 - component recommendations 60–62
 - outbound traffic 174–175
 - separation via firewalls 170–173
- NIST 108–109
- NIST (National Institute for Standards and Technology) 108
- node relationships and interaction 158–159

O

- OLE (Object Linking and Embedding) 40
- OPC (OLE for Process Control) 40
- operating system installation 196
- OSI (Open System Interconnection) 185–186
- outcome of security breach, see impact, security breach

P

- password complexity 79
- patch 47
 - management server 172
- patch management 147–150
- planning and implementation 98
- planning and implementation of a security program 102–107, 116
- policies and procedures 43, 95–96, 103, 117, 118, 119
 - configuration management 126
 - contingency planning 123
 - hiring 120
 - maintenance 126
 - personnel 119
 - physical Environment 120
 - security vendor acquisition 117
- prevention, attack
 - employee training 107
 - encryption 143
 - insider attacks 73
 - intrusion 153
 - risk management activities 110–112
 - twoperson rule 77

- program development 97

R

- RDBMS (Relational Database Management System) 63
- reasons for security 35, 98
- recommendations, network components 60–62
- recovery from attack 124, 125
 - see also backup and recovery
- remote access
 - dial-up modems 140
 - wireless 141
- requirements, operational
 - comparison 38
 - for ICSs 36–37
- resources, additional 19–20, 244–??
- result of security breach, see impact, security breach
- risk areas 35–36
- risks
 - assessing security 40, 113–116
 - managing 108–112
 - poor security 99
 - versus cost to mitigate 107
- rootkit 189
- router 206

S

- SCADA (Supervisory Control and Data Acquisition) 21
- SCADA security recommendations 182
- single endpoint device 163–164, 200
- social engineering 107
 - see also phishing
- software 62–63
- special publications, NIST 108–109
- spyware 67
- steps to manage risk, see managing risks
- suspicious employee behavior 88–89
- system-wide approach 183

T

- TDI
 - ICS security changes below the TDI line 187
 - IT security changes above the TDI line 186
- TDI (Transport Driver Interface) 186
- technical support 20
- third party software demands 160–161
- threats, see attack scenarios
- tools, vulnerability testing 155
- topology, network 25
- training, employee 75–76, 107, 119, 132
- twoperson rule 77

U

- user accounts, timely update 90
- user authentication methods 133–137
- user rights, OS 45
- user rights, Wonderware applications 46

V

virus protection 151–154

VLAN

policy enforcement 140

VLAN (Virtual Local Area Network) 139

VPN

tunnels 198, 223–240

VPN (Virtual Private Network) 145

vulnerabilities

assess 43, 104–106, 113, 155

potential 42, 48–54

W

war dialer 68

Wonderware Security Central website 19

