Pipeline SCADA Security

API STANDARD 1164
SECOND EDITION, JUNE 2009

Pipeline SCADA Security

Pipeline Segment

API STANDARD 1164
SECOND EDITION, JUNE 2009

Special Notes

API publications necessarily address problems of a general nature. With respect to particular circumstances, local, state, and federal laws and regulations should be reviewed.

Neither API nor any of API's employees, subcontractors, consultants, committees, or other assignees make any warranty or representation, either express or implied, with respect to the accuracy, completeness, or usefulness of the information contained herein, or assume any liability or responsibility for any use, or the results of such use, of any information or process disclosed in this publication. Neither API nor any of API's employees, subcontractors, consultants, or other assignees represent that use of this publication would not infringe upon privately owned rights.

Classified areas may vary depending on the location, conditions, equipment, and substances involved in any given situation. Users of this standard should consult with the appropriate authorities having jurisdiction.

Users of this standard should not rely exclusively on the information contained in this document. Sound business, scientific, engineering, and safety judgment should be used in employing the information contained herein.

API publications may be used by anyone desiring to do so. Every effort has been made by the Institute to assure the accuracy and reliability of the data contained in them; however, the Institute makes no representation, warranty, or guarantee in connection with this publication and hereby expressly disclaims any liability or responsibility for loss or damage resulting from its use or for the violation of any authorities having jurisdiction with which this publication may conflict.

API publications are published to facilitate the broad availability of proven, sound engineering and operating practices. These publications are not intended to obviate the need for applying sound engineering judgment regarding when and where these publications should be utilized. The formulation and publication of API publications is not intended in any way to inhibit anyone from using any other practices.

Any manufacturer marking equipment or materials in conformance with the marking requirements of an API standard is solely responsible for complying with all the applicable requirements of that standard. API does not represent, warrant, or guarantee that such products do in fact conform to the applicable API standard.

Foreword

This standard on SCADA security provides guidance to the operators of oil and gas liquids pipeline systems for managing SCADA system integrity and security. The use of this document is not limited to pipelines regulated under Title 49 *CFR* 195.1, but should be viewed as a listing of best practices to be employed when reviewing and developing standards for a SCADA system. This document embodies the API's *Security Guidelines for the Petroleum Industry*. This guideline is specifically designed to provide the operators with a description of industry practices in SCADA security, and to provide the framework needed to develop sound security practices within the operator's individual companies. It is important that operators understand system vulnerability and risks when reviewing the SCADA system for possible system improvements.

Nothing contained in any API publication is to be construed as granting any right, by implication or otherwise, for the manufacture, sale, or use of any method, apparatus, or product covered by letters patent. Neither should anything contained in the publication be construed as insuring anyone against liability for infringement of letters patent.

Shall: The term "shall" is used in this standard to indicate those practices that are mandatory.

Should: The term "should" is used in this standard to indicate:

— those practices for which engineering judgment is required;

— those practices which are preferred, but for which operators may determine that alternative practices are equally or more effective.

This document was produced under API standardization procedures that ensure appropriate notification and participation in the developmental process and is designated as an API standard. Questions concerning the interpretation of the content of this publication or comments and questions concerning the procedures under which this publication was developed should be directed in writing to the Director of Standards, American Petroleum Institute, 1220 L Street, NW, Washington, DC 20005. Requests for permission to reproduce or translate all or any part of the material published herein should also be addressed to the director.

Generally, API standards are reviewed and revised, reaffirmed, or withdrawn at least every five years. A one-time extension of up to two years may be added to this review cycle. Status of the publication can be ascertained from the API Standards Department, telephone (202) 682-8000. A catalog of API publications and materials is published annually by API, 1220 L Street, NW, Washington, DC 20005.

Suggested revisions are invited and should be submitted to the Standards Department, API, 1220 L Street, NW, Washington, DC 20005, standards@api.org.

Contents

Page

Figures

Pipeline SCADA Security

1 Scope

This document is structured so that the main body provides the high-level view of holistic security practices. The annexes provide further details and technical guidance. Reviewing the main body of this document and following the guidance set forth in the annexes assists in creating inherently secure operations. Implementation of this standard, to advance supervisory control and data acquisition (SCADA) cyber security, is not a simple process or one time event, but a continuous process. The overall process could take years to implement correctly depending on the complexity of the SCADA system. Additionally, the process would optimally be started as part of a SCADA upgrade project and use this standard to “design in” security as a element of the new system.

1.1 Purpose and Objectives

The goal of an operator is to control the pipeline in such a way that there are no adverse effects on employees, the environment, the public, or the customers as a result of actions by the operator, or by other parties. This SCADA security program provides a means to improve the security of the pipeline SCADA operation by:

— analyzing vulnerabilities of the SCADA system that can be exploited by unauthorized entities,

— listing the processes used to identify and analyze the SCADA system vulnerabilities to unauthorized attacks,

— providing a comprehensive list of practices to harden the core architecture,

— providing examples of industry best practices.

1.2 Roles and Responsibilities

The operator’s senior management shall implement a program of SCADA security for their organization to identify accountability for all aspects of SCADA security at every organizational level. The SCADA security program scope should include the operator’s organization, business partners, vendors, and external suppliers of SCADA products and services for the SCADA system. The SCADA security program should document the SCADA security plan, identify the roles and responsibilities of security professionals and practitioners who will implement policies and procedures, and provide for the coordination of security efforts in the SCADA domain with the cyber security activities of the entire organization. The SCADA security program shall be designed and communicated so that all personnel who have actual or potential impact on the security of the SCADA system are fully informed of their security roles and responsibilities, and receive adequate training to complete their tasks securely. The SCADA security program should be designed to ensure the organization’s ongoing implementation of industry best practices in cyber security and compliance with all relevant standards.

2 Definitions and Acronyms

2.1 Definitions

For the purposes of this standard the following definitions apply.

2.1.1
access control list
ACL
A list of permissions attached to an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object.

2.1.2
backdoor
trapdoor
A documented or undocumented way of gaining access to a program, online service, or an entire computer system; written by the programmer who creates the code for the program.

2.1.3
biometrics
The study of methods for uniquely identifying humans based upon one or more intrinsic physical or behavioral traits.

2.1.4
confidential
Classification applies to sensitive company information that requires tight/strict security to protect it from unauthorized disclosure, modification, or destruction.

NOTE Unauthorized disclosure, modification, or destruction could have a significant impact. It is information that requires a higher than normal assurance of accuracy and completeness (see Section 6 for more details).

2.1.5
controlled access
Access in which the resources of an area or system is limited to authorized personnel, users, programs, processes, or other systems, and denied to all others.

2.1.6
data center
A facility used to house computer systems and associated components, such as telecommunications and storage systems that generally includes redundant power systems, data communication connections, environmental controls, and security devices.

2.1.7
database management system
DBMS
Computer software designed for the purpose of managing databases based on a variety of data models.

2.1.8
defense in depth
A best practice where multiple layers and types of defense strategies are implemented throughout the SCADA system, which may address personnel, technology, and operations throughout the system lifecycle.

2.1.9
demilitarized zone
DMZ
A DMZ is an intermediary zone between trusted and untrusted networks, providing monitored and controlled access and data transfer (see Figure 3).

2.1.10
deoxyribonucleic acid
DNA
A nucleic acid that contains the genetic instructions used in the development and functioning of all known living organisms.

2.1.11
domain name system
Associates various information with domain names by translating human-readable computer host names into IP addresses.

2.1.12
dual-homed computer
A computer that has network interfaces connected to multiple networks or security domains.

NOTE This is not the same as two network interface cards used for redundancy.

2.1.13
dynamic host configuration protocol
DHCP
A protocol used by networked devices to obtain the parameters necessary for operation in an IP network.

2.1.14
eliminated
To be rid of, or having removed a threat.

2.1.15
enhanced security
Security above the accepted normal level, including, but not limited to, strong or multifactor authentication, encryption, multilevel access control including physical access and biometrics.

2.1.16
extranet
An extranet can be viewed as a part of a company's intranet that is extended to users outside the company. It has also been described as a "state of mind," in which the internet is perceived as a way to do business with other companies as well as to sell products to customers.

2.1.17
facility
A plant, building, structure, or complex contiguously located on the same site, defined by a single geographical perimeter (usually determined by a fence or other barrier that surrounds and limits uncontrolled access), and used by the operator or its contractors for the performance of work under the jurisdiction of the operator.

NOTE The term "facility" includes the land (soil), surface water, and groundwater contained within its geographical perimeter.

2.1.18
file transfer protocol
FTP
An internet standard for transferring files over the internet.

NOTE FTP programs and utilities are used to upload and download web pages, graphics, and other files from your hard drive to a remote server which allows FTP access.

2.1.19
firewall
A set of programs residing on a gateway server that protect the resources of an internal network.

NOTE A firewall examines each network packet to determine whether to forward it toward its destination. A firewall is often installed in a specially designated appliance that is separate from the rest of the network so that no incoming request can get directly at private network resources. At a minimum, a best practice recommendation is stateful or deep packet inspection.

2.1.20
human machine interface
HMI
A computer terminal normally associated with a graphics terminal that allows interaction between people and end devices.

2.1.21
incident response plan
IRP
A plan that identifies and documents the procedures that will be used to detect, respond to, and minimize the impact of a cyber security incident.

2.1.22
information owner
The individual responsible for classification, maintenance, and security of specific data.

2.1.23
instant messaging
IM
A real-time messaging system used to exchange data and information between two or more people across the internet or a corporate intranet.

2.1.24
internal
Information that is accessible to all employees and contractors while providing services to the operator. For operators use only (see Section 6 for more details).

2.1.25
internet control message protocol
ICMP
An extension to the IP defined by RFC 792. ICMP supports packets containing error, control, and informational messages.

NOTE The PING command, for example, uses ICMP to test an internet connection.

2.1.26
internet protocol
IP
A network layer protocol in the IP suite and is encapsulated in a data link layer protocol such as ethernet.

2.1.27
internet service provider
ISP
A company which primarily offers their customers' access to the internet.

2.1.28
intranet
The generic term for a collection of private computer networks within an organization's established policies.

NOTE Intranets generally use standard network technologies like ethernet, TCP/IP, web browsers and web servers.

2.1.29
intrusion detection and prevention systems
IDPS
A more generalized reference to the functions of an IDS and IPS, and reflects the evolving state of these technologies as they are merged into a single family of products.

2.1.30
intrusion detection system
IDS
A type of security management for computers and networks. An IDS gathers and analyzes information from various areas within a device or a network to identify possible security breaches, including intrusions and misuse.

2.1.31
intrusion prevention system
IPS
Supports the ability to receive IDS sensor or scanner data and then apply analytical processes and information to derive conclusions about intrusions, and to execute an appropriate response. IPS-conformant products also provide the ability to protect themselves and their associated data from unauthorized access or modification and to ensure accountability for authorized actions.

2.1.32
IP security
IPsec
A set of protocols developed by the Internet Engineering Task Force (IEFT) to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement VPNs.

NOTE IPsec supports two encryption modes; transport and tunnel.

- — Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched.
- — Tunnel mode is more secure and encrypts both the header and the payload. On the receiving side, an IPsec-compliant device decrypts each packet.

2.1.33
knowledgeable escort
A person who is familiar with the work to be performed by a non-cleared person. This individual must have a solid understanding of the risk involved in the work to be performed. This individual will monitor the work being performed.

2.1.34
layer two (2) tunneling protocol
L2TP
An extension to the PPP protocol that enables ISPs to operate VPNs.

NOTE L2TP merges the best features of two other tunneling protocols: PPTP from Microsoft® [1] and L2F from Cisco Systems® [1]. Like PPTP, L2TP requires that the ISP's routers support the protocol.

2.1.35
local area network
LAN
A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the network.

[1] This term is used as an example only, and does not constitute an endorsement of this product by API.

2.1.36
logical network
The SCADA network and the business network share the same infrastructure and freely route data between the two.

2.1.37
monitoring
The act of observing, carrying out surveillance, and/or recording the presence of individuals for the purpose of maintaining and improving procedural standards and security; including the act of detecting and measuring abnormal conditions.

2.1.38
National Institute of Standards and Technology
NIST
A federal technology agency that develops and promotes measurement, standards and technology.

2.1.39
network file system
NFS
A protocol which allows a user on a client computer to access files over a network.

2.1.40
network news transfer protocol
NNTP
An internet application protocol use primarily for reading and posting usenet articles as well as transferring news among news servers.

2.1.41
operator
A person who owns or operates pipeline facilities.

NOTE For the purpose of this document, the terms "pipeline operator" and "operator" are synonymous.

2.1.42
point-to point-protocol
PPP
A data link protocol commonly used to establish a direct connection between two nodes.

2.1.43
policy
A document that outlines specific requirements or rules that shall be met.

NOTE In the information/network security realm, policies are usually point-specific, covering a single area. For example, an "Acceptable Use" policy would cover the rules and regulations for appropriate use of the computing facilities.

2.1.44
procedure
A documented sequence of activities, steps, decisions or processes, that when undertaken in the sequence provided produces the described result.

2.1.45
process control network
PCN
A network used to transmit instructions and data between control and measurement units and SCADA systems.

2.1.46
programmable logic controller
PLC
A digital computer used for automation of industrial processes.

2.1.47
public
Classification applies to information which is general in nature and can be shared with all individuals for awareness and is not required to satisfy tasks or jobs (see Section 6 for more details).

2.1.48
remote access services
RAS
Any combination of hardware and software that enables the remote access to tools or information that typically resides on a network of SCADA devices.

2.1.49
remote terminal unit
RTU
A remote device typically used to gather status, alarms and analog remote readings for transmission to the SCADA system and transfer controls from the SCADA system to a field device.

2.1.50
restricted
Classification applies to non-sensitive company information restricted to those with legitimate business need for the access.

NOTE Unauthorized disclosure, modification, or destruction could have an adverse impact. This information is intended for use only within the company and in some cases within affiliated organizations, such as company business partners (see Section 6 for more details).

2.1.51
risk assessment
An evaluation of processes for security and safety issues that pose risks to the continuity of safe and reliable operations.

2.1.52
role-based applications
Applications which contain multiple layers of functionality. Authorized users are granted minimal necessary access to the various layers based on job function.

2.1.53
SCADA vendor
Commercial entity or operator that develops and maintains SCADA system software and/or hardware.

2.1.54
secure shell
SSH
A set of commands and protocols that uses digital certificates for authenticating host and client as well as for encrypting communications to ensure security.

2.1.55
secure sockets layer
SSL

Cryptographic protocol that provides secure communications in a network computing environment for such things as web browsing, email, internet faxing, IM and other data transfers.

2.1.56
security domains/security zones

One or more networks isolated from other network(s) by a firewall.

2.1.57
security plan

A set of policies, procedures, or operational requirements, sponsored by management, that outline a multifaceted approach to security issues and related events.

NOTE This approach could include assessments, decision trees, protective mechanisms, responses and recovery, operational security levels, and identified critical assets. A security plan typically considers people, processes and technology.

2.1.58
serial communication

The process of sending data one bit at a time, sequentially, over a communication channel or computer bus.

NOTE Common serial communication electrical interface standards include EIA/TIA 232, 422 and 485.

2.1.59
simple network management protocol
SNMP

A standard TCP/IP protocol for network management used by network administrators to monitor and map network availability, performance, and error rates.

NOTE To work with SNMP, network devices utilize a distributed data store called the MIB. All SNMP compliant devices contain a MIB which supplies the pertinent attributes of a device. Some attributes are fixed or “hard coded” in the MIB while others are dynamic values calculated by agent software running on the device.

2.1.60
strong passwords

A combination of upper and lowercase letters, numbers, and special symbols in a non-predictable order.

2.1.61
superuser do
SUDO

A utility for UNIX® [2]-based systems that provides an efficient way to give specific users permission to use specific system commands at the root (most powerful) level of the system.

NOTE SUDO also logs all commands and arguments.

2.1.62
supervisory control and data acquisition
SCADA

A combination of computer hardware and software used to send commands and acquire data for the purpose of monitoring and controlling (see Figure 1).

[2] This term is used as an example only, and does not constitute an endorsement of this product by API.

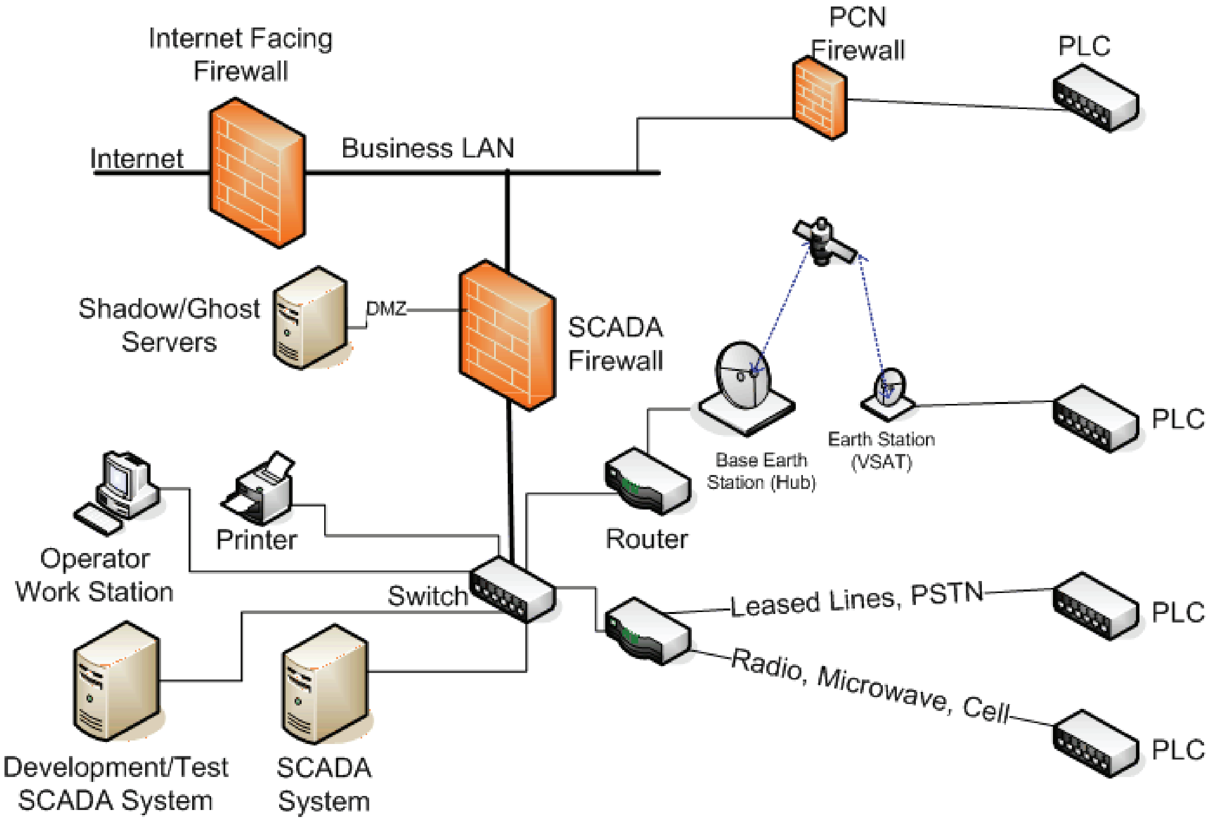

Figure 1—General SCADA Systems Layout

2.1.63
telecommunication center
A facility which houses communication and networking equipment that enables connections between individual end devices, users, and facilities.

2.1.64
third party
Refers to vendors, support personnel, other companies.

2.1.65
transmission control protocol/internet protocol
TCP/IP
TCP is one of the main protocols in TCP/IP networks that enables two hosts to establish a connection and exchange streams of data whereas IP deals only with packets.

NOTE TCP guarantees delivery of data and that packets will be delivered in the same order in which they were sent.

2.1.66
trivial FTP
TFTP
A simple form of the FTP, TFTP uses the user datagram protocol (UDP), provides no security features and is often used by servers to boot diskless workstations, X-terminals, and routers.

2.1.67
utilities
The supply of electric power, water, natural gas, and telecommunications to a control facility.

2.1.68
virtual private network
VPN
A logical, authenticated, encrypted connection that is constructed using untrusted networks that uses encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted and decrypted by unauthorized parties.

2.1.69
voice over IP/IP telephony
VoIP/IPT
A technology that enables the management and transmission of voice calls using an IP network.

2.1.70
vulnerability assessment
An evaluation of technology and system components for any area susceptible to exploitation.

2.1.71
wide area network
WAN
A physical or logical network that provides data communications to a larger number of independent users than are usually served by a LAN and that is usually spread over a larger geographic area than that of a LAN.

2.2 Acronyms

ACL	access control list
BCP	business continuity plan
DBMS	database management system
DHCP	dynamic host configuration protocol
DMZ	demilitarized zone
DNA	deoxyribonucleic acid
DRP	disaster recovery plan
FTP	file transfer protocol
HID	host intrusion detection
HMI	human machine interface
ICMP	internet control message protocol
IDPS	intrusion detection and prevention system
IDS	intrusion detection systems
IEFT	Internet Engineering Task Force
IIS	internet information services
IM	instant messaging
IP	internet protocol
IPS	intrusion prevention system
IPsec	IP security
IRP	incident response plan
ISDN	integrated service digital network
ISP	internet service provider
LAN	local area network
L2F	layer two (2) forwarding
L2TP	layer two (2) tunneling protocol
MIB	management information base

NFS	network file system
NID	network intrusion detection
NIST	National Institute of Standards and Technology
NNTP	network news transfer protocol
PBX	private brand exchange
PC	personal computer
PCN	process control network
PLC	programmable logic controller
PPP	point-to-point protocol
RAS	remote access services
RSA	an algorithm for public-key cryptography, developed by Rivest, Shamir and Adleman (surnames)
RTU	remote terminal unit
SCADA	supervisory control and data acquisition
SMTP	simple mail transfer protocol
SNMP	simple network management protcol
SSH	secure shell
SSL	secure sockets layer
SUDO	superuser do
TCP/IP	transmission control protocol/internet protocol
TFTP	trivial FTP
TIA	Telecommunications Industry Association
UDP	user datagram protocol
VoIP/IPT	voice over IP/IP telephony
VPN	virtual private network
VSAT	very small aperture terminal satellite
WAN	wide area network
WINS	windows internet name service

3 Management System

The operator shall develop a SCADA security management program system with defined policies and procedures that complements and works with the pipeline security plan developed under the guidance of the API's *Security Guidelines for the Petroleum Industry*.

3.1 Personnel

The operator shall develop a personnel security communication and training policy that defines roles and responsibilities, and outlines a training program. This is to ensure that employees and contractors with access to the SCADA system maintain a high level of awareness with respect to potential risks and individual security responsibilities.

Employees and contractors should:

— have an understanding of the nature of information they are handling,

— know how to safeguard the information,

— know how to properly classify the information,

— know how to report and respond to potential threats.

The operator shall develop job responsibilities for key personnel, including system administrators, security coordinators, SCADA support personnel, and controllers. Each employee should be required to follow these job responsibilities.

The operator shall develop a process to ensure that personnel are qualified to manage the SCADA system, and have met company specific security requirements.

3.2 Security Policies

The operator shall develop a set of security policies, executed by a security plan, to ensure safe and reliable operations.

3.3 Risk and Vulnerability Assessment

The operator shall conduct periodic risk and vulnerability assessments. These assessments help ensure safe and secure operations throughout the system life cycle. There are additional external references and guidelines available for use in conducting these assessments.

3.4 Business Continuity Plan (BCP)

A BCP facilitates disruption preparedness and the ability to operate through or recover from an undesirable event. A BCP is part of a security plan and encompasses people, processes, and technology. “People” includes consideration of actions required by key staff during a crisis (response) and after (recovery). “Processes” are critical operations that must be restored to ensure safety and business continuity. “Technology” areas that support those critical processes and foster the response and recovery phase must also be considered. Business continuity and recovery plans should be considered as part of the system availability considerations.

The operator shall establish a BCP to address foreseeable disruptions to the SCADA system, particularly those involving the pipeline control facilities. The BCP should contain the documented recovery objectives that the operator’s management identifies as necessary to maintain safe operation of the pipeline assets. Plans should be included in the BCP to address all the elements required to achieve the recovery objectives. Critical systems backup and restoration procedures shall be put into place to support the BCP.

The operator’s BCP should document the roles and responsibilities of a BCP recovery team. The team should contain all personnel necessary to successfully implement the BCP. The team should test, practice, and refine the BCP recovery process at specified periodic intervals.

A BCP should enable continuous, safe operation of all the operator’s pipeline assets. Because of the many potential risks to individual control facilities, the operator’s BCP shall include a backup control facility capable of ensuring the safe and reliable operation of all pipeline assets in any event that renders the primary control facility inoperable or uninhabitable. Access control should also be considered when preparing for, during, and after a disruption.

Elements of a BCP include a disaster recovery plan (DRP). A DRP includes and identifies essential features and functions, including, but not limited to:

- backup data storage and restoration;
- contact lists for entities such as on call personnel, vendors, service providers and emergency personnel;
- facility maintenance and catering services;
- personnel;
- software licenses;
- specific hardware such as computer platforms, network appliances, printers, fax machines and telecommunication equipment;

— specific software installation media and instructions supporting needs for operating systems and supporting software applications;

— telecommunication service providers, voice and data;

— third-party vendors.

3.5 Incident Response Plan (IRP)

The operator shall establish an IRP to identify and document the procedures that will be used to detect, respond to, and minimize the impact of a cyber security incident. This plan should have input and approval from the operator’s management, as well as all functional teams likely to be impacted by or have responsibilities in response to a cyber security incident. The plan should address all aspects of the planning, response, and recovery phases of the incident. It should include a list of all pertinent roles and responsibilities, as well as specific names and contact information for the members of the incident response team.

A training program should be established for all personnel with responsibilities associated with the IRP. The appropriate periodic testing and evaluation of the IRP should be implemented to ensure a ready, consistent, and documented response to cyber security incidents.

3.6 Change Management

Change management processes define specific policies and procedures for managing changes in installation, configuration, and maintenance of all components of the SCADA system. These systems include, but are not limited to, SCADA hosts, historian servers, programmable logic controller/remote terminal unit (PLC/RTU) and other field devices, human machine interface (HMI) workstations, authentication and network management/monitoring servers, and network infrastructure devices (routers, switches, and firewalls), and their associated operating systems and software. The operator shall develop and communicate a change management plan to manage changes within the SCADA system. The plan should clearly state the operator’s goals in managing change to ensure the availability, integrity and confidentiality of the SCADA system. The change management plan should be reviewed and updated at defined periodic intervals, and whenever organizational, personnel, or technological changes require an update.

The change management plan should establish a baseline configuration standard for all the components of the SCADA system. The baseline configuration should document all information pertaining to the SCADA system component to a level of specificity that would allow the component to be recreated in the time period specified in the operator’s BCP. This baseline configuration should be documented and updated with each approved SCADA system change.

Any planned change to the baseline configuration should include detailed “back-out” or “fall-back” procedures to recover the baseline if the change execution encounters unexpected impacts or failures. Wherever practical, all planned SCADA system changes should be implemented and evaluated in a development or test-bed environment prior to implementation in the production environment.

The change management plan should define the policies and procedures to be used to plan, communicate, document, approve, execute, and review all changes to the SCADA system baseline. The policies and procedures should clearly specify the roles and responsibilities of all personnel involved, as well as the form of documentation and communication that is to be used in the change management. These policies and procedures should be designed to realistically address the operator’s health, security, and safety requirements, staffing and resource constraints, and business operational requirements. The procedures should be carefully scaled to reflect the relative risk to the SCADA system represented by each proposed change to baseline configuration. The review phase of the policies and procedures should include a validation that the change has not compromised the operational performance or the security posture of the SCADA system.

3.7 Operating System and Application Updates

Due to system complexities, operating systems and application software are not inherently secure. In addition, the constant evolution of the computing and networking environment continually reveals new vulnerabilities. To address this issue, vendors publish hot fixes, service packs, and application updates. It is often necessary to apply software hot fixes and updates to maintain system stability and security, but the risk of applying patches and updates to real-time systems should always be weighed against the risk posed by the present vulnerabilities. Operational and SCADA security concerns require that certain precautions be taken when applying software modifications:

— install only SCADA vendor approved software;

— any update should be certified by the SCADA vendor before being applied to the SCADA system;

— updates should be analyzed for applicability in your environment;

— if possible, documented installation procedures for updates should be obtained from the SCADA vendor;

— updates should never be applied directly from the internet;

— an offline test environment should be utilized to test updates before being applied to a production environment;

— applicable functionality testing should be performed before modified system builds are moved into production environments;

— once system modifications are complete, a security compliance checklist should be reviewed to ensure the SCADA system still complies with the operator's security policies.

For the purpose of this document, operators who develop and maintain SCADA systems in-house are considered a SCADA vendor. These procedures should be performed in accordance with the operator's change management plan.

3.8 Application and Software Restrictions

SCADA networks are designed primarily to support proprietary control systems using efficient protocols with low bandwidth requirements and limited tolerance for transmission delays. Since these networks are dispersed over wide geographical areas, with historically expensive wide area network (WAN) connections, they have often been designed with minimal bandwidth specifications. For this reason, the addition to the SCADA network of any additional protocols, applications, or communicating software packages should be approached with great care to preserve the unimpaired availability of the SCADA system. No additional protocols, applications, or software should be added to the SCADA networks that are not essential to pipeline operations or for the maintenance of the SCADA network infrastructure. Commercial business software and information services such as internet access should not be made available on the SCADA network. System event or alarm notifications using email type applications shall be outbound only with proper security applied. No software or application should be added to the SCADA network that could create unmonitored liability for copyright infringement or legally-defined offensive content. Any new protocol, application, or software proposed to be added to the SCADA network should be run in a test-bed or development environment to evaluate the potential for impairing the performance of the SCADA system, particularly with regard to bandwidth requirements, since modern servers and software packages can easily consume WAN capacity at the expense of critical SCADA traffic.

4 Physical Security

Operators of critical transportation infrastructure shall take measures and controls to deny unauthorized persons access to control facilities. Some of the measures for good control room physical security are outlined under the following sections. For further information, please refer to API's *Security Guidelines for the Petroleum Industry*.

The operator shall develop and maintain a security policy and associated procedures that require all personnel with access to the SCADA facilities to undergo periodic security reviews.

The operator shall develop and maintain a security plan for operator-controlled utilities that supply the control center operation. These utilities include, but are not limited to, power distribution systems, uninterruptible power supplies (UPS), and power generation equipment.

The operator shall develop and maintain a security plan for all operator-controlled SCADA network infrastructures. The operator should secure the access to all network and computing ports and deactivate any unused ports.

The operator shall perform a risk assessment of all operator-controlled facilities where SCADA equipment resides and shall develop a process for controlling access to that equipment. The operator should consider installing intruder detection into unmanned sites such as valve sites, pump station, metering facilities, etc. Unauthorized personnel shall be escorted by authorized personnel when accessing SCADA facilities.

5 System Access Control

System access control deals with user accounts, authentication, and authorization. The following sections will identify requirements and discuss several issues that are unique to SCADA systems.

5.1 Restricted Access

Multilayer access and multifactor authentication have a greater chance of preventing system compromise than a single layer system. In a multilayer system, the failure of one layer does not compromise the entire system because each layer functions independently. The use of a defense in depth multilayer security system can greatly reduce the probability of a system compromise.

5.2 User Accounts

SCADA systems typically have two layers of user accounts; the operating system layer, such as a UNIX® [3] or Windows® operating systems, and an application layer, for user specific rights within the SCADA application. An access control list (ACL) to either layer shall be maintained. A valid business reason should exist before granting persons access to the SCADA system or resources. Accounts should be implemented so that data access is limited only to user required data.

5.3 Operating System Accounts

Access to the operating system “sysadmin” account allows total control of a workstation. Any file or device on a workstation can be modified or deleted. Access to the sysadmin account should be strictly controlled. Only individuals requiring the capabilities this account provides should be given the access. In operating systems like UNIX® [3], the use of a tool like superuser do (SUDO) can provide some of the functionality of the sysadmin (root) account without the full privileges. Other operating systems have similar tools to provide similar functionality.

SCADA operation consoles must remain logged on at all times to properly monitor pipeline operations. The use of shared operating system accounts for operating consoles that are used 24 hours a day/seven (7) days a week is acceptable. These consoles are generally protected by physical security and are manned 24 hours a day/seven (7) days a week. The use of these shared user accounts should be reviewed regularly and restricted to specific console operations.

[3] This term is used as an example only, and does not constitute an endorsement of this product by API.

SCADA vendors sometimes use or create operating system accounts to allow them to monitor and maintain the SCADA system. These accounts may provide easy access for intruders. All operating system accounts shall be secured and use strong passwords or biometrics.

Some operating systems and/or applications use internal accounts. These accounts generally have significant access to the operating system. These accounts should be reviewed to ensure appropriate levels of security are set up to prevent unauthorized users from using these accounts.

5.4 SCADA Accounts

All users of a SCADA system application should have a unique account that requires a password or biometric methods to access the system. Unique accounts help to track unusual activity on a system.

Some operators do not utilize individual operator accounts due to the potential operational risk. Operators should seek to employ processes that minimize operational risks while considering alternative operator login procedures that could improve system security. All non-console SCADA accounts should use enhanced security.

The use of inactivity timers for workstations/personal computers (PCs) that are not used for operating purposes should be considered. These timers will log off users who may have left their terminal for more than a specified amount of time.

5.5 Password Controls

A strong password scheme is a cornerstone of a good security system. Some attributes of a strong password scheme include:

— expiration periods;

— minimum length requirements for passwords;

— prohibition of reuse of passwords, usage of common words, usage of numeric or alpha patterns;

— requirement that passwords be case-sensitive;

— lockout after a certain number of failed attempts;

— replacement of default and initial account passwords on initial login.

All systems/equipment should implement as many of these features as possible. Computer systems provide many tools and techniques to simplify day-to-day activities, including script files, aliases, and shortcuts. Care shall be taken to insure that passwords are not embedded into these tools, because intruders can read these files and use the passwords to manipulate the system. SCADA source code may also have hard coded passwords. The SCADA security policy should discourage/prohibit the embedding of sensitive passwords in source code, scripts, aliases, and shortcuts. If necessary, encryption techniques should be used. All source code should also be secured to minimize other users' access to embedded passwords. Passwords should be entered by the user at each login rather than stored for automatic login.

5.6 Biometrics

Biometrics is the application of using uniquely recognized human based attributes based on one or more intrinsic physical or behavioral traits to obtain access to secure sites, information or applications. Some examples of biometrics include:

— physiological—face, fingerprint, hand geometry, iris, deoxyribonucleic acid (DNA);

— behavioral—keystroke, signature, voice.

There are several reasons to use biometrics within SCADA and process control network (PCN) systems such as:

— positive identification of a specific individual (supposedly),

— convenience—no badge or password or security token device to carry around.

Biometrics can be a valuable second input where multifactor authentication makes sense and supports the defense in depth concepts. Biometrics techniques such as thumb print recognition could be applied in place of user account/ password access controls.

Biometrics contributes to cyber security when properly applied but biometrics controls are not infallible; they can be compromised. Research has shown that fingerprint, iris, and retinal scans all have high likelihood of circumvention. Biometrics is an emerging technology. Implementation strategy, cross-over error rates, platform availability should be considered prior to usage.

5.7 Disabled Non-required Services

Operating system services which are not used by the production SCADA system should be removed or disabled to reduce the risk of being used as an attack mechanism. Services may be running by default when the operating system is installed on a server but not used by the SCADA system. These services should be disabled to prevent their in appropriate use. Other services should be analyzed using a risk assessment to see if the benefits of having them running outweigh the potential for exploitation. Examples of operating system services which are commonly disabled are:

— automatic updates,

— dynamic host configuration protocol (DHCP) server,

— distributed file system,

— DNS client,

— file transfer protocol (FTP) service,

— IIS admin service,

— indexing service,

— instant messaging (IM),

— network file system (NFS),

— network news transfer protocol (NNTP) service,

- remsh,
- rexec,
- simple mail transfer protocol (SMTP),
- telnet,
- windows internet name service (WINS),
- world wide web publishing service.

5.8 Operating System Tools

The remote shell, remote login, and remote copy functions of operating systems like UNIX®[4] allow "trusted" connections between workstations. If this functionality is available, an individual who has successfully logged on to one workstation can access all other workstations on the network. The remote functions that an operating system provides should only be used when necessary. This functionality should be disabled for most users. In cases where remote functions are required, the use of tools such as a secure shell (SSH) can improve the security of these functions.

FTP allows files to be sent or received on a workstation/PC. Without proper security, an intruder could use this tool to install programs that allow them to take control of a workstation/PC. The use of FTP on a SCADA system should be strictly controlled. The sysadmin account should not be granted FTP capability. In cases where FTP functions are required, the use of secure tools can improve the security of these functions.

Access to any SCADA function in an operating system environment is typically provided through a shell or window. Besides the intended function, a shell or window can be used as an access point into the rest of the SCADA system. The use of a secured shell or window tool and good account design will limit access to other parts of the system.

5.9 Device Access

There are many devices on a network besides workstations and PCs, such as network switches, routers, firewalls, and terminal servers. In the field, this can also include transmitters, PLCs, flow computers, etc. Many of these devices have factory default passwords or null passwords. These devices can also be manipulated by intruders to gain access to a SCADA system. Devices that have the capability should be secured with a strong password and shall not use the default password provided by the vendor. Changing the ID or account to something different from the vendor's default for these devices should also be considered.

5.10 Personnel Administration

While this topic is covered in the management system section, it is important to reiterate that as part of a security plan, policies exist that require review of accounts on a SCADA system and/or device shall be reviewed and audited on a regular basis. Likewise, policies should also exist that require departing employees or contractors to be addressed immediately.

6 Information Distribution

The sharing of certain types of information could increase the potential for inappropriate access and misuse of the SCADA system. Therefore, it is recommended that all types of information about the SCADA system be analyzed and classified, according to the operator's security plan and procedures, before it is shared. It is equally important to determine what types of information can be shared with each individual based on their job/role. When confidential/

[4] This term is used as an example only, and does not constitute an endorsement of this product by API.

restricted information must be shared with third-party personnel, confidentiality agreements, background screening, and training/awareness of security procedures should be considered.

The operator shall follow company established policies for handling information.

It is recommended that a minimum of three levels of classification should be used for SCADA information. The operator shall determine the levels to use based on the following guidelines:

— confidential,

— restricted,

— public.

6.1 Confidential

Confidential information should only be shared with personnel on a need-to-know basis. Access to confidential information should only be used in order to meet the requirements of a job or task. Confidential information is information that is not widely shared and that is highly protected. Specific details regarding the SCADA system are classified as confidential information. Information classified as confidential should be protected in the best manner.

The following items are examples of confidential information (this is not meant to serve as a complete list):

— access rule sets,

— addressing schemes,

— PLC register layouts,

— system schematics,

— system configurations,

— user account information.

6.2 Restricted

Restricted information may be specific, and although it can be shared with a larger number of individuals than confidential information, it is still protected. Restricted information is shared for awareness and to meet job or task requirements, but not for general knowledge.

The following items are examples of restricted information (this is not meant to serve as a complete list):

— communication media,

— communication protocols used,

— equipment lists,

— security plans.

6.3 Public

Public information is general in nature and can be shared with all individuals. Public information is shared for awareness and is not required to satisfy tasks or jobs.

Due to the critical nature of SCADA systems, minimal information pertaining to the system should be classified as public. SCADA information classified as public should go through a review by the appropriate management to assess the risk of the release.

7 Network Design and Data Interchange

In the past, SCADA systems were typically isolated and ran independently of other business functions and applications. However, as technology has advanced, interconnectivity has become commonplace. There is an advantage for business systems to have access to SCADA data. The following sections will address achieving secure system interconnectivity.

7.1 Network Design

There are many methods that can be used to link SCADA systems to corporate business systems. However, these connections should be limited to specific services or devices and shall be secured. It is important to note that connecting any device to the PCN requires an evaluation of risk to the network as well as the risk to the device being connected.

7.1.1 Interconnected Business and SCADA Networks

This can be an installation where the SCADA systems and the business system share the same logical network or where the traffic is openly routed between the two networks (see Figure 2). This makes the SCADA system vulnerable to deliberate and unintentional user attacks. The operator shall plan to isolate the SCADA network.

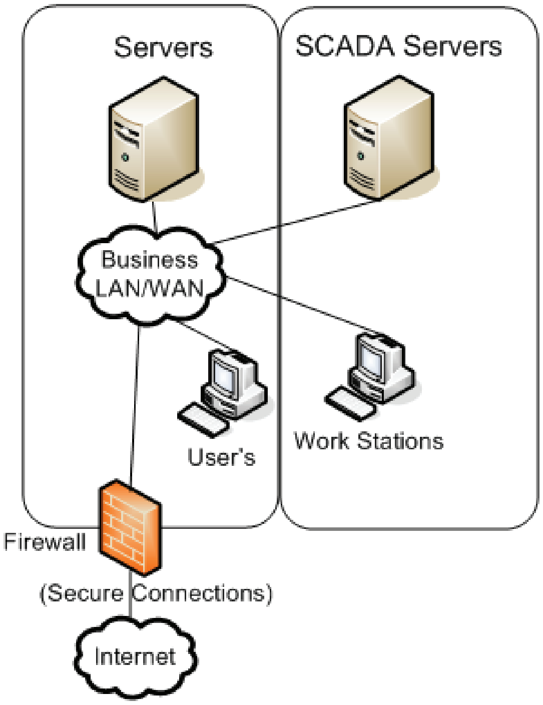

Figure 2—Typical Non-isolated Implementation—Not Recommended

7.1.2 Communication Demarcation Points

A physically secure location should be provided for communication demarcation points to minimize access by unauthorized personnel.

7.1.3 Firewalls

A monitored and maintained firewall provides perimeter defense at the network layer and at the application layer. A firewall shall be used when connecting the SCADA network and business network. The firewall shall be configured to block all unnecessary access and allow only essential traffic approved by the security policy (see Figure 3).

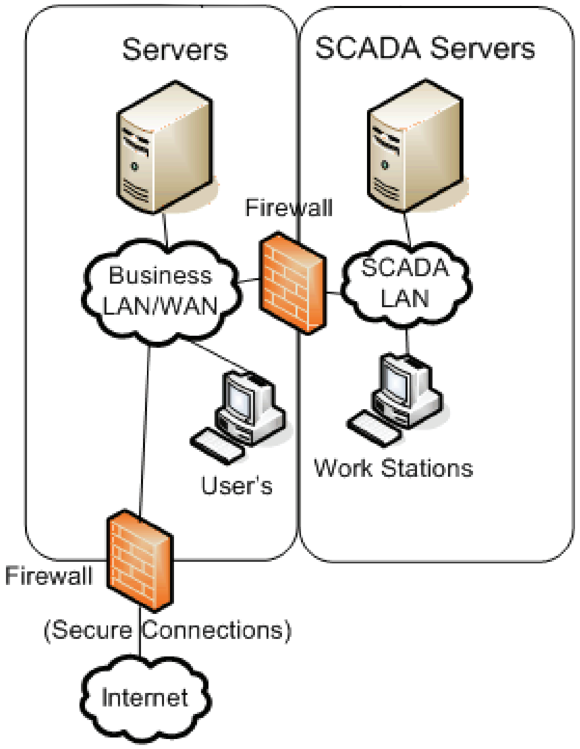

Figure 3—Typical Firewall Isolation Implementation—Minimal Isolation

7.1.4 Demilitarized Zone (DMZ)

A DMZ is a separate network that is placed between the SCADA network firewall and the business network firewall (see Figure 4). Computers or other equipment that must communicate with both networks are placed in the DMZ network. This ensures there is no direct communication between the SCADA network and the business network.

7.1.5 Dual-homed Computers

Dual-homed computers that connect two different security domains (other than dedicated firewalls) shall not be implemented within the SCADA network. Unless functioning as a dedicated firewall, a dual-homed computer has the potential to bypass network security isolation (see Figure 5).

7.2 Network Management

Management of networks requires up-to-date documentation and diagrams on how the network is designed and how it is intended to operate. Network management processes should be aligned with the overall change management plan.

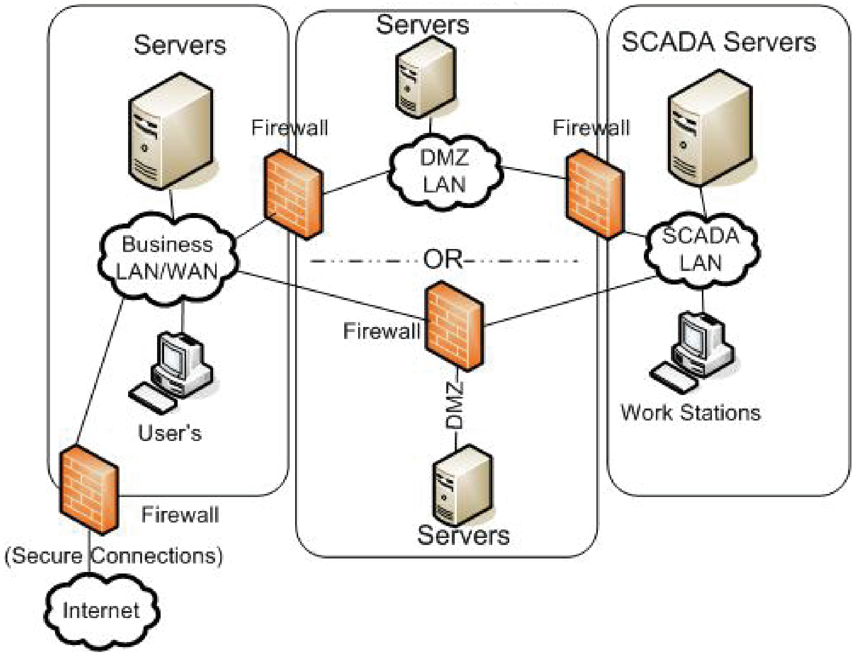

Figure 4—Typical DMZ Implementation—Recommended

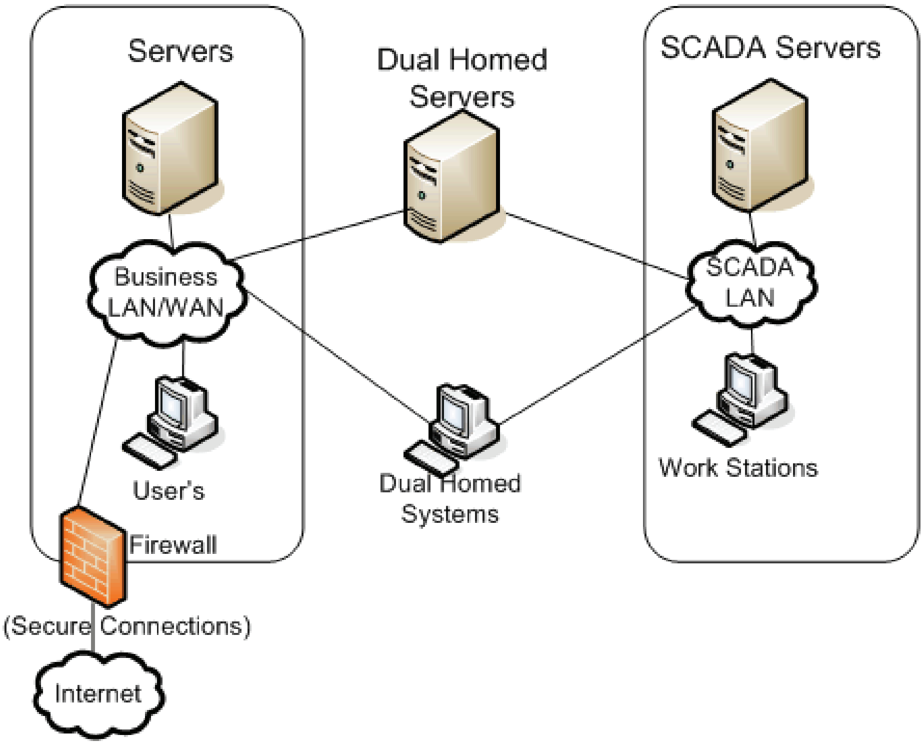

Figure 5—Typical Dual-homed Computer Bridge Implementation—Not Recommended

The operator should ensure that configuration files used to program network devices (such as routers, switches, firewalls) are properly archived, and that those archives represent what is in production. The operator should regularly review versions of software running within those network devices, and review and assess any known vulnerabilities, with the intent to remediate as required.

The operator should manage the network by monitoring network traffic and general activity, avoid the use of unmanaged devices, and monitor network usage and traffic patterns. The operator should periodically review network log files, error messages, and other events to track potential security breaches or other anomalous activity.

The process of managing network devices can be enhanced by appropriate tools.

7.2.1 Network Monitoring

While no universally accepted best practices exist for network monitoring in a SCADA or control system, implementing a combination of technologies in addition to firewalls is necessary to enhance network security and management. Transmission control protocol/internet protocol (TCP/IP)-based networks have become the underlying enabler of connectivity based on industry standards. This relative ease of use presents many challenges in network management and security.

Beyond the implementation of technology, generated data should be reviewed on a regular basis, as defined in the security plan. Failure to do so will not achieve any significant improvement in management or security. The aggregation and correlation of information from multiple sources, and the necessity to present it in a meaningful manner can be an onerous task and can be assisted by appropriate tools.

7.2.2 Network Security

In addition to the implementation of firewalls, traffic monitoring, and event logging, technologies that focus on specific security exposures should be considered. Two areas that are significant are:

— intrusion detection and prevention, and

— file audit and control.

7.2.2.1 Intrusion Detection and Prevention Systems (IDPS)

The operator should evaluate the use of the IDPS to monitor the behavior of network to identify events that may be considered unusual or undesirable. Methods to employ the IDPS include:

— network monitoring, where network segments or devices are examined for suspicious activity in network and application protocols (also referred to as NID—network intrusion detection);

— wireless, where wireless network traffic is examined for suspicious activity in the protocols;

— behavioral or heuristic, where the network is examined for unusual traffic flow;

— host monitoring, where a host computer is examined for suspicious activity (also referred to as HID—host intrusion detection).

Due to the nature of SCADA traffic (which is generally considered to be different from more traditional business systems), and unique protocols that may be implemented, the use of the IDPS should be carefully examined to ensure that safe and reliable operation of the system being controlled is not compromised by automated actions of the IDPS. The intrusion detection system (IDS) should be implemented and reviewed well in advance of enabling the intrusion prevention system (IPS).

7.2.2.2 File Audit and Control

The operator should monitor files and log changes to preserve SCADA system and data integrity. Monitoring of files not expected to change (including operating system, application, and configuration files) should be performed such that changes are detected and logged. The process of managing auditing and control of files can be enhanced by appropriate tools.

7.3 Data Interchange

Connections between the SCADA network and other networks are being driven by many business needs. If the SCADA security program allows these connections it is acknowledged that they pose a significant cyber security risk. This risk shall be analyzed and appropriate precautions implemented according to the security program guide lines. As part of this implementation, policies and procedures should be developed and agreement reached on how the company and external organizations should respond if a SCADA system security risk is identified.

7.3.1 Connections Between the SCADA Control Center Operational Facilities, Data Center, and Telecommunications Center

It is recommended that wherever possible the control center operational facilities should be located as closely as possible to the SCADA data services and telecommunication services. System designs should ensure that the SCADA operators are never without the ability to connect to the SCADA system and the SCADA servers are not cut off from the telecommunication connections to remote pipeline locations.

7.3.2 Connections Between the SCADA System and Business Networks

The use of SCADA and PCN data by corporate entities other than operations has become more the rule than the exception. Consideration shall be taken to ensure the data and network used by production remain reliable and not be affected by corporate data acquisition activities. Systems accessed by entities other than operations should do so from a separate system than that of operations. A separate security zone or subnet, such as a DMZ, should be used to replicate system data and securely provide data to corporate data consumers. Appropriate network security measures should exist between the production SCADA and replication systems, in the form of firewalls, DMZs and other appropriate network devices.

7.3.3 Connections Between the SCADA System and Business Partners SCADA Systems

In many situations, it is necessary for one company’s SCADA system to communicate control data to another company’s SCADA system. These data include, but is not limited to, shutdown requests, measurement information, valve status, etc. This information can be transmitted many different ways, such as host-to-host, PLC-to-PLC, etc. When this type of communication is required, the operators shall mutually develop a secure method of communication.

7.3.4 Connections to Third Parties for Support

It is important that third-party personnel be able to support the systems they sell, and in some cases they will require access to the SCADA system for this purpose. Methods for third-party access to the SCADA system include access via an extranet, internet, modem, etc. Third-party connections should be controlled and secured with an authentication method. A secure method shall be established and monitored according to the operator security policy.

Internet access is sometimes needed for vendor support of the SCADA system. This access should be controlled via firewalls and other security devices. Access should be granted to a secure corporate network initially, then access granted to the SCADA system from there. System analyst oversight is necessary to remove access rights given to the vendor once the work has been completed. A firewall shall be used to isolate the SCADA network from the internet.

7.3.5 Internet and Business Network Access

SCADA system assets shall not be used to access business network resources or the internet. The preferred method for accessing untrusted resources is to provide a separate workstation, specifically for business usage, such as email or internet browsing, connected to a network segment not associated with the SCADA network or PCN.

7.3.6 Voice Over IP/IP telephony (VoIP/IPT)

Businesses have been implementing VoIP systems as a method of reducing communication costs. While VoIP is not recommended for use on SCADA systems there are situations where a physical communications circuit is shared with non-SCADA users. In addition, VoIP may be used within the SCADA network to provide mission critical services. If VoIP usage is required as described above, it shall be implemented with additional control measures for securing and segregating the voice traffic. VoIP traffic should not be allowed to supersede SCADA traffic.

7.3.7 Instant Messaging (IM)

Businesses are using IM as a business critical communication tool. Risks associated with IM systems included spyware, trojan horse programs, viruses, worm attacks, spam and loss of critical and corporate information. Internet-based IM systems should not be allowed on a SCADA system. If company policy requires the use of IM, the company shall take control measures to prevent the IM system from interfering with the SCADA system. Monitoring systems should be implemented to protect against these risks. If IM is required but only used for communication, file sharing should be disabled, if possible.

7.3.8 Wireless Networking

The role of wireless networking should be carefully evaluated and assessed for risk before implementation. Wireless networking has an elevated level of security concern for PCN and/or SCADA systems. For this reason, a risk assessment should be completed to weigh the benefits of implementing wireless networking against the potential risks for exploitation. These technologies have the potential to propagate SCADA system data over an indeterminate geographic distance which transcend any local physical security. Good network management practices, such as encryption and firewall segmentation should be applied to wireless networking. Additional wireless networking control technologies should be considered. These may include, but are not limited to, the use of secure protocols, enhanced authentication, tunneling, and controlling access points.

Physical access control to wireless equipment is necessary. Additionally, network infrastructure should be secured to prevent the unauthorized introduction of wireless technology. Wireless connectivity should be included in network documentation, policies, and procedures. Wireless networking technology changes frequently and security depends on the ability to stay current and protected.

7.3.9 Audio/Video Conferencing

Audio and video conferencing can be a good way to connect with remote personnel and to better facilitate the exchange of ideas for business purposes. However, due to security concerns and bandwidth required for audio and video conferencing, they should not be utilized within the SCADA communications network.

In the event that audio and/or video conferencing is required within the SCADA communication network, measures should be put in place to limit its impact on SCADA information. Such measures might include data prioritization for SCADA operations, bandwidth limitation assignments for the conferencing data, or other quality of service measures that will limit the impact to the SCADA operations within the infrastructure. No audio or video conferencing traffic should traverse any process control firewall due to the increased exposure to security vulnerabilities.

7.3.10 Video Surveillance

Video surveillance can be considered a special type of SCADA data and is used to monitor security and enhance safety of remote locations. In the event that video surveillance is required within the SCADA network; measures should be put in place to limit its impact on SCADA operations. Such measures might include data prioritization for non-video SCADA information, bandwidth limitation assignments for the surveillance data, or other quality of service measures that will limit the impact to the SCADA operations within the infrastructure. Video surveillance data should be protected as indicated in Section 6 of this document. Proper controls should be in place when transferring video surveillance data between security zones.

8 Field Communication

Communication plays a special role in a successful SCADA system. Beyond providing the basic connectivity methods, the communication system provides confidentiality, integrity and availability of data streams. SCADA communication is moving away from serial-based dedicated leased line or dial-up methods in favor of IP based services. The SCADA communication connection is typically the long communications path from the control center to the remote device. Utilizing telecommunications external to the control center exposes the system to unauthorized monitoring or tampering. The following sections will highlight the unique aspects of a SCADA communication system.

8.1 Field Device Technology

Field devices provide the SCADA system with an interface to industrial devices that are designed to provide analog and status information from transducers and sensors. These signals are converted to digital values and transmitted upon request using various methods of telemetry. Commands are transmitted to the field devices and are processed in a similar manner. Certain classes of field devices such as PLCs, flow computers, engine/motor safety devices, and electrical equipment, provide specific functionality. These devices can pose an operational risk if compromised.

Field devices may have local or remote access for configuration, calibration, and programming. This creates security problems because the field devices do not generally have the capability required to secure network connectivity. For this reason, all security controls recommended in this document should apply to these devices.

A partial list of security controls include the following.

- Passwords should be unique for each instance of the device that exists and changed in accordance with the operator’s password management policy. Vulnerabilities exist when serial ports provided by equipment makers are not protected by passwords or when the default passwords are used.

- When practical, field devices should utilize enhanced authentication, including multilevel user authorization. If this capability is not available, precautions should be incorporated for external protection of communication ports.

- The operator interface panels should incorporate password protection to prevent unauthorized individuals from accessing the interface.

- The operator should require the field devices to have internal logic that protects the facility it is controlling. If unauthorized commands are received, the field devices should react in a fail-safe manner to protect the facility.

- Configuration software and development tools for field devices offer limited security. Device access should require enhanced authentication. Physical security should be provided and maintained for the field device enclosure.

- Software development, upgrades, and change management of these devices should follow security requirements outlined in 3.6.

8.2 System Access

The SCADA system is often connected to various entities, both internal and external to the SCADA network. This section discusses various interconnections and associated best practices.

8.2.1 Network Protocols

TCP/IP is becoming the protocol of choice for interoperability of host and field devices. Unnecessary services [such as simple network management protocol (SNMP) and trivial FTP (TFTP)] should be disabled. Where services like these need to be used, the default user names and passwords should be changed to complex read/write strings and strong passwords. Non-secure protocols such as telnet and FTP should be replaced with secure alternatives, where possible.

8.2.2 Encryption of Data on Accessible Paths

Connectivity between field and SCADA systems should be encrypted. Secure encryption technologies can be applied to reduce risks to data confidentiality, integrity, and availability. Using the internet for field data communications is not recommended. If the internet is the only feasible connection, encrypted secure connectivity shall be used to connect the field location to the SCADA system. Prior to incorporating any encryption method, an analysis should be performed to ensure that the enhanced security does not interfere with the proper operation of the SCADA system.

8.2.3 Casual User Access to Network

Unauthorized workstations should be prohibited from connecting to the network. Unused network ports should be disabled.

8.2.4 Remote Access to SCADA Components

Remote access to SCADA components such as HMI, PLC, RTU, etc., should only be enabled when necessary and approved using strong authenticated. These measures should require enhanced cyber security measures to compensate for the absence of physical security. When feasible, additional industry best practices for secure remote connectivity should be considered.

8.2.5 Dial-up Modem Access for Maintenance

Any dial-up modem used for maintenance purposes should require enhanced security. Callback and authentication servers are desirable enhancements due to the fact that modems are inherently difficult to secure. dial-up modems should be disconnected from the network when not required. The use of dial-up modems should be minimized.

Annex A
(informative)

The following list is compiled from the written text of API 1164 and from best practices in the industry, and should be used by the operator as a guide when reviewing their SCADA systems for appropriate level of protection. This annex is by no means an all-inclusive list, and is not intended to cover all possible security vulnerabilities in SCADA systems.

Security Plan and Procedure	**In-place/ Required/ Not Needed**	**Verified by:**
Are security plans, policies and procedures in place that address people, processes, and technology?		
Have critical assets and operational functions been identified and agreed upon at the organizational level?		
Are priorities clearly identified at all levels of the organization? These include safety, compliance, physical and information security, etc. Are these considered throughout the security plan?		
Are roles and responsibilities for management and schedules for review and if required updating of the security plan clearly delineated?		

Information Retention/Archive/Backup Standards	**In-place/ Required/ Not Needed**	**Verified by:**
Data contained in applications is subject to the information retention requirements set forth in the company's information retention policy. Operators shall consider these retention requirements when they develop off-site backup rotation and retention schedules for each application that they support, based on requirements set forth by the operator and the records retention schedule. This schedule shall reflect the risk assessment of the information being stored.		
The system administrator shall ensure that all data are backed up according to the requirements of the operator and the records retention schedule. File/database servers shall have at a minimum an incremental backup performed at least daily, and a full backup performed weekly. Copies of backups shall be sent off-site. It is the responsibility of the system administrator to ensure that the system can be restored and available to meet the business requirements as defined by the information owner.		
Operators shall document backup and recovery procedures based on the requirements of the information owners.		
Information systems data classified as restricted or confidential shall be backed up daily and stored in a suitable off-site location as defined in the information retention policy.		
Information systems data classified as public shall be backed up periodically, as determined jointly by the operator and information custodian, and periodically moved to a secure location.		

Information Retention/Archive/Backup Standards (Continued)	In-place/ Required/ Not Needed	Verified by:
Information custodians of application systems are responsible for documenting and maintaining software and hardware recovery procedures.		
Software includes, but is not limited to, any program/application/system required to reconstruct the processing environment.		

Business Continuity Planning	In-place/ Required/ Not Needed	Verified by:
Each organization with mission-critical and/or restricted or confidential data shall develop and maintain a current BCP.		
Operator shall determine the availability requirements of their information systems. This determination relies on analyzing the impact to the organization, and how quickly the system must be recovered.		
The operator is responsible for maintaining, testing, documenting, and executing a DRP. This DRP is a component of business continuity and must encompass data backup and recovery procedures, and software and hardware recovery procedures.		
A BCP shall be reviewed and updated at least annually in order to be current.		
The time frame for resuming system processing in the BCP/DRP is consistent with business requirements and recovery strategies.		
Operators shall perform tests of the restoration process at least annually following successful implementation of a backup and restoration process or if there is a change in the components of a backup process (source, media, equipment, logical routing, etc.). Only the operator may authorize personnel (information custodians, system administrators) to recall backups and perform restores.		
The plan shall include an inventory of all systems software necessary and sufficient to reconstruct the processing environment and to support critical applications.		
Each reporting unit shall test their BCP/DRP on an annual basis. This test must be documented and the results reported to the operator and any other committee that is designated by company management.		
Restoration testing shall be performed with live production backup data on the test systems in the test environment only.		
Copies of the BCP/DRP and backup software (data and system) shall be kept in an off-site storage facility.		
Alternate, manual processing methods shall be identified and documented in the plan for continuing operations while the environment is being recovered.		

Business Continuity Planning (Continued)	In-place/ Required/ Not Needed	Verified by:
The plan shall include, but not be limited to, provisions for a contingency facility and hardware equipment. The contingency facility should be a fully operational facility configured to the reporting unit's specifications.		
The BCP/DRP shall include availability and location of alternate system hardware.		
Dependencies and recovery processes related to third-party vendors [i.e. internet service provider (ISP), utility, or telephone companies] shall be identified and incorporated into the BCP/DRP.		
Hardware includes but is not limited to any central processing unit (CPU), memory unit, peripheral, remote terminal, controller, communication equipment and/or line, printer, and any other related items of hardware required to reconstruct the processing environment.		
System and application software backup shall be performed before system upgrades and/or maintenance occurs.		
Tape backups of all information classified as restricted or confidential shall be sent off-site to a remote location at intervals specified in the BC/DRP.		
Processes shall exist to incorporate changes, like software or hardware updates, to the system environment in the BCP/DRP.		
The plan shall include alternative options based on the type of disaster that occurs.		
The plan shall identify and address network and other application dependencies if they exist.		
The plan shall include provisions, schedules, responsibilities, and tracking for the training and skill development of the people that are required to be at the recovery site to restore the system and its data. The recovery team must include business owners and users of the system. The team shall include alternates who are also fully trained in rebuilding the system.		
The plan shall include procedures for requesting off-site backup media.		
Communication procedures for recovery team members to use after the disaster, during recovery, and after recovery shall be documented.		
Users of the system shall participate in testing of the BCP/DRP to ensure the system works as intended.		

Change, Configuration and Problem Management Standards	In-place/ Required/ Not Needed	Verified by:
The operator shall ensure development and documentation of change control procedures.		
Change requests for applications and/or systems that contain restricted or confidential information shall be documented via a reporting unit approved change request form. The change request form must, at a minimum contain the following information: — who is initiating the change, — who is responsible for implementing the change, — who is responsible for the approval, — business justification for the change, — nature of defect (if applicable), — estimated resource requirements necessary to complete the change, — testing required and who is responsible for the testing, — back-out procedures, — systems impacted, — user contact information.		
The operator must approve change requests.		
A limited number of factors may make the required change process prohibitive (e.g. a limited number of employees). In these instances, develop mitigating controls and request an exception.		
Change management standards shall include control procedures to address emergency conditions within the SCADA systems and supporting networks that would pose a threat to health, safety or the environment.		
All emergency requests shall be documented after implementation. Documentation must include such activity as the account of the person(s) making the change, time, date, commands executed, program and data files affected, etc. The person(s) making the emergency change must also provide a written description of what was done to address the emergency to the appropriate operator.		
The operator is responsible for monitoring the installation of emergency fixes. In rare cases where programmers need update access to the production environment, special temporary accounts or access will be created. These temporary accounts must be disabled or deleted upon completion of the emergency session.		
The roles and responsibilities for individuals involved in the change control process shall be clearly defined and documented. Incompatible responsibilities must be segregated (i.e. programmers responsible for coding changes must not move these same changes into production).		
Application developers shall not have write access to the production environment and production executable code.		

Change, Configuration and Problem Management Standards (Continued)	**In-place/ Required/ Not Needed**	**Verified by:**
Applications shall have separate controlled environments for: — development/staging, — integration and user acceptance testing, — production source (where applicable), — production executable code.		
Operator shall ensure identification and documentation of conditions (types of changes) that require compliance with these detailed change control procedures (i.e. high-risk version upgrades vs low-risk maintenance).		
Operator shall maintain documentation of change control procedures.		
In small shops where separation of duties and a test environment may not be practical, mitigating controls can be developed. The exception process should be utilized for these cases.		
All SCADA system source code and configuration files shall be restricted to authorized support personnel only.		
There shall only be one repository for production source code. Developers shall retrieve the source code from this repository when modifying programs. All modifications to production source code must be documented for proper version control.		
The access privileges of developers to production libraries shall be restricted such that they will only be permitted to copy source code from production into their development area and write or move modified code into a staging library.		
A change control process shall be in place to ensure that programmers are adequately restricted from accessing production and testing environments.		
All information is subject to operators information retention schedules.		
All applications shall be integration tested (e.g. testing interdependencies to ensure they do not disrupt other functions) prior to implementation of the software into the company production computing environment.		
Any data used for testing shall comply with information protection standards.		
The user acceptance plan of applications shall include tests of all major functions, processes, and interfacing systems. Testing procedures shall be documented.		
During user acceptance testing, logical access restrictions shall ensure that developers have no update access and that the code being tested cannot be modified without notification to the information owner.		

Change, Configuration and Problem Management Standards (Continued)	**In-place/ Required/ Not Needed**	**Verified by:**
All non-emergency changes to company computer networks shall follow company change and problem management standards. Changes to company internal networks include, but are not limited to: — loading new network software, — changing network addresses, — reconfiguring routers, — adding dial-up lines, — creating trusted host relationships.		

Operating System and Application Standards	**In-place/ Required/ Not Needed**	**Verified by:**
New operating systems and application implementations should incorporate security measures in the development stage. Security measures shall be tested before new operating systems and applications are placed into the production environment.		
Operating system and application update procedures are in place.		

Application and Database Standards	**In-place/ Required/ Not Needed**	**Verified by:**
Applications and databases shall not have means of gaining unauthorized access (“backdoors”).		
Operator shall perform an analysis of applications and databases to determine criticality, data sensitivity, and application type. This determination will identify whether baseline requirements are sufficient or if the additional critical/sensitive requirements shall be applied. Categorize data sensitivity as: — confidential, — restricted, — public.		
New applications and databases, whether in house custom designed or commercial off the shelf, will incorporate security measures, as established by the security policies and procedures, beginning in the development stage. Security measures shall be tested before these applications and databases are placed into the production environment.		
Compliance is required for all applications and databases, in-house developed, or vendor purchased/developed.		
All role-based applications require unique user accounts and strong passwords that provide user authentication that supports the capability to enforce role separation.		

Application and Database Standards (Continued)	In-place/ Required/ Not Needed	Verified by:
Application user accounts shall be protected. Do not store user accounts and passwords in the database tables unless absolutely necessary. If it is necessary to store passwords in the database tables, then encrypt the passwords.		
Database administration privilege (delete, insert, select and update) access shall be limited to the operator's authorized database administrator role.		
All access to restricted or confidential data through analytical or utility applications that lack access controls shall to be managed through the operating system and/or database access control functions.		
Role-based applications require access authorization procedures and/or access control processes for restricted or confidential data. Access shall be consistent with the user's job responsibilities.		
End-users shall not have the capability to access the application code or databases from outside the controls of the application. This access shall be restricted to authorized personnel only (i.e. system or application support personnel).		
All users shall be identified and authenticated prior to being granted data access from the application or database.		
Role-based applications or applications accessing restricted or confidential data shall limit administrative access to the least privileged basis acceptable for completing administrative duties.		
"Superusers/All" access accounts shall be limited to only administrators that need unlimited access in order to meet a business need.		
Executables shall be restricted from unauthorized executions or alterations.		
As a guideline, applications should force non-operator users off after 15 minutes of inactivity, where possible. The user shall be re-authenticated before access is restored.		
Each operator shall ensure there is documentation for using and administering mission-critical applications.		
Each operator shall ensure there is system and program documentation. This includes, but is not limited to: — hardware and software configuration, — database design and structure including logical and physical database schemas, — maintenance and modification procedures.		
Each operator shall ensure a backup and recovery plan is documented consistent with the business requirements.		
All data shall be entered by authorized users. Segregation of duties shall be maintained.		

Application and Database Standards (Continued)	In-place/ Required/ Not Needed	Verified by:
Data validation and integrity (e.g. business rules) shall be implemented commensurate with business requirements.		
The application shall be the only method for data entry, deletion, or update. If data entry, deletion, or update to the data is required outside the controls of the application, then the change and problem management standards apply.		
Updates to imported files shall not be permitted. Controls shall exist to prevent unauthorized updates to files that will interface from one production environment to another.		
The application shall have internal controls implemented to ensure data are correctly and accurately processed.		
Confidential data shall be securely transmitted using necessary encryption in accordance with the encryption section under computer, telephone and network usage standards.		
Only system accounts (those defined and used only by the application or operating system) shall be able to run background jobs.		
Establish interface/transfer controls and procedures shall be established to ensure data loss or corruption is detected and corrected.		

Physical Security Standards	In-place/ Required/ Not needed	Verified by:
Company information in any format (hard copy, disk, tape, etc.) shall be protected by all employees and contractors at a level commensurate with its value.		
All servers running or housing confidential data shall reside in secure data centers, where available, or secured data rooms.		
Media, including computer hard drives, containing confidential level information shall be stored in an access restricted environment (i.e. vault, data centers, hotel safe).		
All information stored on media is assumed to be classified as public and does not need to be labeled as such. All other classifications of information (restricted and confidential) shall be appropriately labeled on the media.		
Immediately following permanent or temporary relocation, a work team shall be assigned to perform a final sweep and inspection of all vacated work areas and furniture to ensure that no information assets remain. Care shall be taken to assign responsibility for all common areas (e.g. hall file cabinets, file rooms, closets, storage rooms, etc.).		
Following permanent and temporary relocations all network ports and all telephone lines shall be disabled immediately following relocation unless continued activation is authorized by the customer currently paying for the network port and phone line.		

Physical Security Standards (Continued)	In-place/ Required/ Not needed	Verified by:
During workspace location changes, all inventory control documentation shall be updated to reflect the changes made.		
All SCADA computing, telecommunication, and networking centers should be monitored continually [24 hours a day/seven (7) days a week]. This monitoring can be done by cameras, alarmed doors and windows, people manning the centers, or a combination of the above.		
Each SCADA control center should have a set of operating procedures to protect equipment contained within. These procedures should include, but not be limited to, consideration for the following: — fire prevention, — fire detection, — fire suppression, — shutdown procedures, — natural disasters, — terrorism, — utilities (power and water), — vandalism, — water detection.		
SCADA control centers should be equipped with doors that automatically close immediately after they have been opened, and which set off an alarm when they have been kept open beyond a period of 30 seconds.		
SCADA control centers should be equipped with surveillance cameras to monitor entrances to the control center.		
Fire walls surrounding SCADA control centers should be non-combustible and resistant to fire for at least one (1) hour. All openings to these walls (doors, ventilation ducts, etc.) should be self-closing and likewise rated for at least one (1) hour.		
Physical access to magnetic tape, disk, and documentation libraries shall be restricted to workers whose job responsibilities require access to these locations.		
All information storage media (such as hard disk drives, floppy disks, magnetic tapes, and CD-ROMs) containing confidential data shall be physically secured from unauthorized access when not in use. An exception will be made if this information is protected via an encryption system that complies with the encryption standards.		
Access to all unused physical ports on computer and network equipment should be deactivated. This includes ethernet ports on switches, routers, and firewalls as well as universal serial bus (USB) ports on servers.		
Buildings that house company computers or communications systems shall be protected with physical security measures that prevent unauthorized persons from gaining access to the building.		

Physical Security Standards (Continued)	**In-place/ Required/ Not needed**	**Verified by:**
Physical access to all rooms containing company computer systems, wiring or communications equipment [wiring closets, private brand exchange (PBX) rooms, etc.] shall be locked at all times with access restricted to authorized personnel only. Owners of this equipment shall maintain a list of individuals authorized for access and review this list on a twice-annual basis.		
All employees, contractors, and visitors on company premises shall carry identification tags at all times. Lost cardkeys or equivalent access authorization device shall be reported within 24 hours to the applicable local security officer.		
Access shall be revoked immediately, in no case later than 24 hours, once the access is no longer needed. It is the responsibility of the immediate supervisor to see that cardkeys are retrieved and cancelled for terminated or transferred employees and contractors.		
Authorized personnel shall not allow unknown or unauthorized individuals into restricted areas without an escort. Personnel without a valid reason for being in the computer room shall be escorted out of the computer room immediately and appropriate security personnel contacted.		

Authentication Standards	**In-place/ Required/ Not needed**	**Verified by:**
User accounts may only be established with documentation via a form that identifies: — the identity of the user, — who has authorized the addition of the user account.		
User accounts shall be disabled upon termination of employment.		
User accounts shall be reviewed and a process in place to disable if inactive for more than 90 days if appropriate.		
Each computer and communication system user account (excepting only mandatory administrative accounts) shall uniquely identify only one user. Shared or group user accounts are not the desired state but can be permitted for the console. Users are also not allowed to share their password with anyone else.		
Each computer and communication system user account shall be unique and forever connected solely with the user to whom it has been assigned. After an employee or contractor leaves the company, there shall be no re-use of any user accounts associated with that employee or contractor, unless reassigned to the same person.		
Users are responsible for all activity performed with their personal user accounts. User accounts may not be utilized by anyone but the individuals to whom they have been issued. Users shall not allow others to perform any activity with their user accounts.		

Authentication Standards (Continued)	In-place/ Required/ Not needed	Verified by:
Users with privileged access (system administrators) shall be assigned a separate, unique account, different from their non-privileged account. Company information systems shall use a naming convention for privileged user accounts consistent with the domain owner's user identifier standards.		
Where possible, (operating system dependent) users with access to superuser or privileged accounts (system administrators) shall use their personal account to log into systems. Administrators shall then switch the current account to the privileged account as required.		
Users with privileged access (system administrators) will use special privileges only when acting as administrators; they will use their non-privileged user accounts with limited privileges for normal work. Where possible, the administrator will log in with their non-privileged user accounts and then upgrade to privileged account as required.		
The use of superuser/administrative accounts that are not uniquely assigned to an individual shall be limited to only those situations absolutely necessary to maintain pipeline operations.		
Complexity rules shall be implemented within the operating system functionality. If a system has no password complexity functionality (or it is insufficient), then a password filter or other compensating control shall be implemented.		
General users and administrators: — password expiration: 90 days, — eight (8) character minimum length, — passwords shall be composed of a combination of letters and numbers and can include symbols, — password history capabilities shall be enabled and the last 12 encrypted passwords stored per user.		
Service account (host-to-host data transfer accounts): — password expiration: when an individual who knows the password changes roles, — 14 character minimum length, — passwords shall be composed of a combination of letters and numbers and symbols, — when the system capability exists password history shall be enabled and with the last 12 encrypted passwords stored per user.		
If operating system platforms or applications support encryption, then password files shall be protected and encrypted.		
Passwords in transit shall be encrypted within the packet or transmitted over an encrypted conduit [like secure sockets layer (SSL)].		
Default passwords of applications, operating systems, database management systems (DBMSs) or other programs shall be changed immediately after installation.		

Authentication Standards (Continued)	In-place/ Required/ Not needed	Verified by:
The combination of a company account and password shall not be used for authentication on external internet sites.		
Initial and reset login passwords shall follow password complexity rules and require the user to immediately change the password.		
When creating strong passwords avoid using the following when creating a strong password. — Words easily associated with the company, account owner ID, address or user name. — Dictionary words or proper nouns. — Calendar combinations, e.g. jan2001, feb2001, etc. — Sequential numbers with words, e.g. word0001, word002, word003, etc., or 001word, 002word, 003word, etc. — Passwords that are too similar. Make at least three characters totally different from the previous password. — Repeated patterns or palindromes, e.g. aaa1aaa.		
Users are the owners of their passwords. As such, they: — shall not share their passwords with others; — shall not write down the password in any available place; — shall be aware of their surroundings and of situations where the password could be gleaned from observation, etc.; — shall not embed passwords into files/scripts.		
One user password change per system or application per day is permitted.		
Computer system administrators shall create initial user passwords that are a minimum of eight (8) characters in length and are comprised of letters, numbers, and special characters (where technically possible).		
Initial passwords shall not be easily associated with the company or the user (i.e. social security number, employee number, address, numerical equivalent of name, etc.).		
Where technically feasible, new users shall be forced by the system they are accessing to change their initial password to one that meets password standards.		
All default passwords delivered with hardware and software shall be changed with installation to meet with company password standards.		
The use of a pass phrase code in which one letter, number, or symbol from each word in the phrase is used in the password is a good practice.		
For non-operator consoles, upon five (5) consecutive authentication failures, users will be locked out of the resource in which they are attempting to gain access.		

Authentication Standards (Continued)	In-place/ Required/ Not needed	Verified by:
Users shall demonstrate a justifiable business case in order to obtain permission from the information owner to access SCADA data.		
When the operator grants users access to SCADA data, such authorization shall be documented via a form that identifies: — who is requesting access, — what they are requesting access to, — who has approved the access.		
Operator shall ensure intended recipients of that information have the right and need to know the information being provided before granting access. The right to know principle can be equated to a justifiable business case. If the user needs access to the information to fill a bona fide business need then that user will be given access.		
Data and information shall not be used, accessed or operated upon except by authorized employees and/or contractors in their assigned work and responsibility on a need-to-know, need-to-see, or need-to-use basis.		
Operators are responsible for reviewing system privileges on a semiannual basis and shall promptly revoke all privileges no longer required by users, including system administrators. Reviews shall be performed on a semiannual basis due to the ever-changing business environment and the importance of the data. It is the responsibility of system administrators to ensure that operators are provided with the proper reports to review all user access.		
Access privileges shall be reviewed upon employee transfer or job reassignment.		
The operator shall remove access to information as soon as that access is no longer needed. It is the responsibility of both the user and the operator to see that access privileges are aligned with the needs of the business and are assigned on a need-to-know basis.		

Personnel Security Standards	In-place/ Required/ Not needed	Verified by:
The human resources department shall facilitate secure and confidential information handling policies when introducing new individuals to the company. All new employees shall receive a copy of the information security policies and/or security awareness materials appropriate for their position and role within the company and acknowledge that they understand their responsibilities as stated in the policies and standards.		
A personnel security communication and training policy that defines roles, responsibilities, condition of employment, hiring screening processes, and outlines a training program is in place.		

Personnel Security Standards (Continued)	**In-place/ Required/ Not needed**	**Verified by:**
Each reporting unit shall establish and maintain a process to record all employees and contractors access to information systems and data, as well as, assigned company property, including, but not limited to: — access badges, — credit/calling cards, — keys, — laptops/desktops, — personal digital assistants (PDAs), — phones, — remote access.		
The supervisor or manager shall notify all operators that have granted access to information systems or data to promptly revoke such access in the case of terminations, or revoke/modify such access in the case of transfers.		
The supervisor or manager shall collect any items issued to the employee, contractor, or third party such as laptop computers, software, data, documentation, manuals, smartcards, handheld devices, etc.		
When users with access to confidential or restricted information are transferred or terminated, the employee's supervisor or contractor's sponsor shall directly coordinate with operator the date for removal of the users' access rights. If the user is to be fired, then access shall be revoked BEFORE the user is notified of the termination.		
For situations in which users with access to data centers are transferred or terminated, the employee's supervisor or contractor's sponsor shall notify local security to ensure access to the protected areas is revoked.		
When an employee leaves any position with the company, the department manager shall review both computer resident files and paper files to determine who will become the custodian of such files.		
Physical access controls shall be implemented for company facilities where information assets are stored. These controls shall be consistent with company policy—security of personnel and assets.		

Information Classification and Application Criticality Standards	**In-place/ Required/ Not Needed**	**Verified by:**
All production information within the company will have a designated Information owner. The information owner's responsibilities are detailed in the information protection roles and responsibilities standards.		
Operations shall compile and maintain a data repository catalog or high-level description of confidential and restricted information. This catalog shall be reviewed and updated annually.		

Information Classification and Application Criticality Standards (Continued)	In-place/ Required/ Not Needed	Verified by:
Information cannot be downgraded to a lower classification without undergoing a risk assessment effort sponsored by the information owner.		
Operator shall assign application criticality and data sensitivity classifications.		

Network Connectivity Standards	In-place/ Required/ Not needed	Verified by:
A DMZ shall be established between the company's trusted, private network and the internet.		
Both host- and network-based IDSs should be deployed in the DMZ.		
Two traffic-filtering devices (i.e. router and firewall) should be used in succession to filter inbound and outbound traffic and to restrict access to only those resources required.		
Monitoring should occur for traffic traversing from an un-trusted to trusted zone.		
Third-party access shall be restricted to only the resources necessary to meet the business need.		
A switch shall not be configured to simultaneously manage internal, DMZ, and external traffic.		
Network architecture shall be designed to minimize the possibility that a single point of failure would prevent any critical system from fulfilling its function.		
With the exception of kiosks, all users shall authenticate to the network before gaining access to any network resources.		
SCADA computers should be periodically audited and updated for security patches and hot-fixes.		
All network device ACLs shall be documented. Documentation shall include the purpose of each rule, interdependencies, and security considerations addressed.		
Where security requirements have not been defined, no connections are allowed without explicit, documented review and approval.		
All wireless networks shall be properly secured.		
All remote access into the SCADA system shall be approved prior to implementation.		
All remote access into the SCADA system shall use strong authentication.		
Operators shall maintain a list of users with remote access.		

Network Connectivity Standards (Continued)	In-place/ Required/ Not needed	Verified by:
Remote systems shall not be configured to automatically connect to the SCADA system without authentication input from an authorized user.		
Periodic reviews should occur to identify unauthorized access to SCADA system.		
Periodic reviews should occur to ensure network documentation is current.		

System Security Audit and Review Standards	In-place/ Required/ Not needed	Verified by:
Logs containing computer or communications system security relevant events shall be retained for a period as defined in the information retention policy. Logs shall be secured to prevent modification. Only authorized personnel are allowed to review these logs. These logs are important for error correction, security breach recovery, investigations, and related efforts.		
All company employees shall watch for, and promptly report, any potential security incidents including viruses, intrusions, and out-of-compliance situations immediately using company incident reporting, escalation, and resolution procedures.		
User access activity records shall be kept for those users that access restricted or confidential information in accordance with the requirements set by the company's information retention policy. The operator will review these records on a monthly basis and these records shall be maintained.		
The operator is responsible for monitoring and logging system activity for the purpose of discovering security events. Only authorized individuals with prior management approval will evaluate and/or use network testing/monitoring software or hardware.		

Contractors, Vendors, Consultants, and Third-party Standards	In-place/ Required/ Not Needed	Verified by:
All contracts related to information security services and products shall meet all applicable operators' security policies.		
Approval from the operator shall be obtained if the services provided by contractors may or will affect confidential information.		
The manager responsible for the contract with the contractor shall ensure that the contract specifies compliance with all policies and actions to be taken for violations.		
The ownership of software developed by contractors shall be defined in the contract agreement.		
Contractors that access company information shall be contractually bound to uphold the operator's information security policies. Approval of the contractual language shall be obtained from the operator's legal department.		

Contractors, Vendors, Consultants, and Third-party Standards (Continued)	In-place/ Required/ Not Needed	Verified by:
The operator shall periodically review a contractor's compliance with the operator's information security policies.		
Contractors shall be subject to access restrictions required to fulfill the conditions of the contract.		
Each contracting company and employees thereof, performing services for the operator shall sign a non-disclosure agreement according to the operator's security policies.		

Computer and Network Usage Standards	In-place/ Required/ Not Needed	Verified by:
Personal use of SCADA computing and communication resources should not be permitted.		
The use of operator's SCADA computing and communications resources for the following activities is prohibited: — unethical or illegal activities, — attempting to access information not authorized to view, — unauthorized disclosure of confidential or restricted information, — any other activities prohibited under the operator's security policies.		
Virus scanners and/or detection programs should be installed when their application does not cause disruption or negative impact on the SCADA system operation. If they are not used, other measures should be taken to isolate or protect the system from viruses.		
Any files from outside the SCADA system shall be scanned and verified for viruses and authenticity before installation or execution. External storage media should be scanned and verified before use.		

Computer, Telephone, and Network Usage Standards	In-place/ Required/ Not Needed	Verified by:
Before being given the opportunity to log in to any operator SCADA computer, users shall be presented with a login banner according to operator's security policy, or a banner that states: — the SCADA system is to be used only by authorized users; — by continuing to use the SCADA system, the user represents that he/she is an authorized user; — use of the SCADA system constitutes consent to monitoring. The following is an acceptable form of a login banner in U.S. locations: "This SCADA system is for use by authorized users only. Any individual using this system, by such use, acknowledges and consents to the right of the company to monitor, access, use, and disclose any information generated, received, or stored on the systems, and waives any right of privacy or expectation of privacy on the part of that individual in connection with his or her use of this system. Unauthorized and/or improper use of this system, as delineated by corporate policies, is not tolerated and the company may take formal action against such individuals." Non-U.S. locations may have specific laws that regulate system usage and monitoring. Legal departments in non-U.S. locations should review the login banner wording, modify banner wording to comply with local laws, and document any modifications. Legal reference responsible for the modification to the banner shall be cited. System administrators are responsible for implementing the login banner and any modifications.		
Identification of the operator, system specific information, network, location, or host shall not appear prior to a successful login.		
Systems shall be configured not to provide any information on an unsuccessful login. This includes identifying which portion of login sequence (user account or password) was incorrect.		
When using encryption it should be applied using the most secure industry standard methods compatible with the SCADA system.		
Restricted or confidential information should be encrypted when stored or transmitted outside of the SCADA system.		
The operator shall comply with operator's policy for information retention and the company's records management program that set forth retention and destruction schedules and requirements for company business records.		
Electronic information storage media shall be disposed of in a manner commensurate with the highest information classification stored upon the media.		
All electronic media that has stored confidential information should be physically destroyed if, at the time of disposal of the media, that information is still considered confidential.		
All electronic media that has stored restricted information should be at least degaussed or wiped if, at the time of disposal of the media, that information is still considered restricted. If media cannot be degaussed or wiped, the media shall be physically destroyed.		

Computer, Telephone, and Network Usage Standards (Continued)	In-place/ Required/ Not Needed	Verified by:
PCs/laptops outside the SCADA security controlled areas shall not be left unattended without invoking a terminal lock or password protected screensaver. Operating systems that allow the workstation to be locked, and thereby providing the same level of protection as an operating system that requires authentication prior to boot-up, are acceptable.		
PCs/laptops and servers outside the SCADA security controlled areas, when possible, should be configured with a password protected screen-saver. The screen-saver shall require the entry of a password after a PC/laptop or server console has been left idle for 10 minutes.		

Annex B
(Example)

SCADA/Control System Security Plan

This document is intended to be used as an example for developing an operator-specific SCADA security plan and was compiled using the DOE's *21 Steps to Improve Cyber Security of SCADA Networks*, API 1164 and industry best practices. This annex is by no means an all-inclusive list, and is not intended to cover all possible security vulnerabilities in SCADA systems.

Revision History

Date	Description	Revision Number	Approver
10/01/03	Document released for approval	1.1	Manager

B.0 Introduction

Each business unit shall use this SCADA/control system security plan to develop a specific security plan.

A list of the 21 steps in the DOE document is provided below for reference.

This document is broken into five sections. These sections are:

— "Identification and Documentation,"

— "Risk Analysis,"

— "Preventive Action,"

— "Oversight,"

— "Security Management."

The first three sections describe the steps necessary to identify, conduct a risk assessment and take the preventive action necessary to secure the SCADA/control system. The oversight and security management sections describe the methods that should be used to ensure the long term security of the SCADA/control system and how the SCADA/control system security should be managed.

This document includes a two-page summary of these sections to give a brief overview of this document. The summary lists the key points but does not give the detail provided in the individual sections.

DOE's 21 Steps to Improve Cyber Security of SCADA Network

1) Identify all connections to SCADA networks.
2) Disconnect unnecessary connections to the SCADA network.
3) Evaluate and strengthen the security of any remaining connections to the SCADA network.
4) Harden SCADA networks by removing or disabling unnecessary services.
5) Do not rely on proprietary protocols to protect your system.
6) Implement the security features provided by device and system vendors.
7) Establish strong controls over any medium that is used as a backdoor into the SCADA network.
8) Implement internal and external IDSs and establish 24-hour-a-day incident monitoring.
9) Perform technical audits of SCADA devices and networks, and any other connected networks, to identify security concerns.
10) Conduct physical security surveys and assess all remote sites connected to the SCADA network to evaluate their security.
11) Establish SCADA "Red Teams" to identify and evaluate possible attack scenarios.
12) Clearly define cyber security roles, responsibilities, and authorities for managers, system administrators and users.
13) Document network architecture and identify systems that serve critical functions or contain sensitive information that require additional levels of protection.
14) Establish a rigorous, ongoing risk management process.
15) Establish a network protection strategy based on the principle of defense-in-depth.

16) Clearly identify cyber security requirements.

17) Establish effective configuration management processes.

18) Conduct routine self-assessments.

19) Establish system backups and DRPs.

20) Senior organizational leadership should establish expectations for cyber security performance and hold individuals accountable for their performance.

21) Establish policies and conduct training to minimize the likelihood that organizational personnel will inadvertently disclose sensitive information regarding SCADA system design, operations, or security controls.

B.1 Identification and Documentation

B.1.1 Each [COMPANY] unit will identify and document the SCADA/control systems network connections and architecture. Each unit identifies systems that serve critical functions or contain sensitive information that require additional levels of protection.

Documentation generated in this section or any of the following sections should be considered sensitive and is NOT for general distribution. Each document needs to be handled as sensitive in accordance with items in 6.2.

Information collected in this section should be referenced as an annex, but not distributed with the plan.

NOTE Develop and document robust information security architecture as part of a process to establish an effective protection strategy. It is essential that organizations design their networks with security in mind and continue to have a strong understanding of their network architecture throughout its lifecycle. Of particular importance, an in-depth understanding of the functions that the systems perform and the sensitivity of the stored information is required. Without this understanding, risk cannot be properly assessed and protection strategies may not be sufficient. Documenting the information security architecture and its components is critical to understanding the overall protection strategy, and identifying single points of failure.

B.1.1.1 Identify, document and develop a comprehensive understanding of all connections to the SCADA/control systems.

B.1.1.1.1 Identify the connections to the SCADA/control system.

— Identify the locations that communicate with another location.

— Identify the connections at each location that communicate or could be used to communicate outside that location.

— This would include phone line modems, lease line modems, integrated service digital network (ISDN), frame relay, very small aperture terminal satellite (VSAT), radios, fiber optic transmitters, hardwire direct connection, wireless ethernet transmitters, connections to the internet and/or any other communication method that can be used to communicate to another location.

— Identify if this communication is between devices within the [COMPANY] SCADA/control system or to an outside entity.

— Shippers, venders/systems integrators, [COMPANY] business devices, etc.

— Identify the connections within the location that communicate to any devices outside the SCADA/control system.

— [COMPANY] business devices, etc.

— Identify the connections within the location that communicate with an outside entity.

— Business partners, PLCs, etc.

— Identify if these connections are normally active or inactive.

— Identify the type of communication used for the connections identified above.

— Master/slave, slave/master, peer to peer, asynchronous or IP, protocol, etc.

— Identify the methods used to make a connection outside the SCADA/control system.

— DMZ PLC, firewall, dual-homed computers, direct connections, etc.

B.1.1.1.2 Determine the purpose and necessity of the connection.

— Identify the connections absolutely necessary for the operation of the control system.

— Identify the connections required for regulatory requirements.

— Identify the connections used for business partner data exchange that is used for control.

— Identify the connections used for business partner data exchange that is not used for control.

— Identify the connections used to provide control system data to business applications.

— Identify the connections needed to maintain that control system.

— Identify the connections no longer necessary or not used.

B.1.1.1.3 Identify the location of the physical access point into the SCADA/control system.

— This is normally going to be an ethernet connection such as a hub or a switch or any wall jacks that can be used to access the ethernet network of the SCADA/control system.

— Other access points that do not use ethernet should be identified and analyzed to see if someone could gain access to the SCADA/control system from that point.

B.1.1.1.4 Identify how well the connection and access point is protected.

— Identify the software security measures in place for the connections.

— Identify the physical security measures in place for the access points.

— Identify the connection and its vulnerability to unauthorized connections.

B.1.1.2 Identify and document the equipment that is connected to the SCADA/control systems network.

B.1.1.2.1 Identify the location of each piece of equipment that is connected to the SCADA/control systems network.

B.1.1.2.2 Identify if it is SCADA/control systems equipment, business systems equipment or a third-party's equipment.

B.1.1.2.3 Identify the category of the equipment:

- local area network (LAN) communications (hubs, switches, routers, firewalls);
- WAN communications (routers, modems, radios);
- domain controller;
- SCADA server;
- HMI;
- file server;
- PLC or other controller device;
- historical server;
- maintenance/monitoring;
- other server;
- other device.

B.1.1.2.4 Identify what type of connection the equipment has and the protocol used:

- ethernet,
- TCP/IP,
- serial,
- modbus,
- etc.

B.1.1.2.5 Identify if the equipment is critical to the SCADA/control system.

B.1.1.2.6 Identify if the equipment contains critical data.

B.1.1.3 Conduct physical security surveys and assess all remote sites with connections and access points into the SCADA/control system network to evaluate their security.

NOTE Any location that has a connection to the SCADA network is a target, especially unmanned or unguarded remote sites. Conduct a physical security survey and inventory access points at each facility that has a connection to the SCADA system. Identify and assess any source of information including remote telephone/computer network/fiber optic cables that could be tapped; radio and microwave links that are exploitable; computer terminals that could be accessed; and wireless LAN access points. Identify and eliminate single points of failure. The security of the site must be adequate to detect or prevent unauthorized access. Do not allow "live" network access points at remote, unguarded sites simply for convenience.

B.1.1.3.1 Evaluate the access points to the SCADA/control system for its physical security.

— Unmanned remote facility access points need to have some form of physical security. They should be locked inside a building or inside a box that has a fence around it with a locked gate.

— In manned facilities, the access should be in a limited access location that is monitored for unauthorized access.

— In main office buildings, each access point needs to be in a locked or secured room.

B.2 Risk Analysis

B.2.1 Each [COMPANY] unit will do a security risk analysis and establish a risk management process.

NOTE A thorough understanding of the risks to network computing resources from denial-of-service attacks and the vulnerability of sensitive information to compromise is essential to an effective cyber security program. Risk assessments form the technical basis of this understanding and are critical to formulating effective strategies to mitigate vulnerabilities and preserve the integrity of computing resources. Initially, perform a baseline risk analysis based on a current threat assessment to use for developing a network protection strategy. Due to rapidly changing technology and the emergence of new threats on a daily basis, an ongoing risk assessment process is also needed so that routine changes can be made to the protection strategy to ensure it remains effective. Fundamental to risk management is identification of residual risk with a network protection strategy in place and acceptance of that risk by management.

B.2.1.1 Conduct a risk to benefit analysis of each connection to the SCADA/control system.

B.2.1.1.1 During the analysis do not rely on proprietary protocols as a means of protection.

NOTE Some SCADA systems use unique, proprietary protocols for communications between field devices and servers. Often, the security of SCADA systems is based solely on the secrecy of these protocols. Unfortunately, obscure protocols provide very little “real” security. Do not rely on proprietary protocols or factory default configuration settings to protect your system. Additionally, request that vendors disclose any backdoors or vendor interfaces to your SCADA systems, and expect them to provide systems that are capable of being secured.

B.2.1.1.2 Examine the connection and determine its overall risk and give it a risk ranking (1—low risk, 5—high risk).

Each business unit will develop and document the criteria for assigning the risk ranking.

A risk is defined as the vulnerability a connection has to being compromised (i.e. a connection to the internet is a high risk, a serial connection between local devices is a low risk).

B.2.1.1.3 Examine the connection and determine its overall benefit and give it a benefit ranking (1—low benefit, 5—high benefit).

Each business unit will develop and document the criteria for assigning the benefit ranking.

— Examine the connection and determine its overall benefit to the control system.

— Examine the connection and determine its overall benefit to operations.

— Examine the connection and determine its overall benefit to maintenance.

— Examine the connection and determine its overall benefit to customer service.

— Examine the connection and determine its overall benefit to [COMPANY].

B.2.1.1.4 Compare the benefit of each connection to its risk and give it an overall ranking (1—high risk/low benefit, 5 —low risk/high benefit).

Each business unit will develop and document the criteria for assigning the overall ranking.

B.2.1.2 Conduct a risk analysis of the equipment used in the SCADA/control system.

B.2.1.2.1 Examine the pieces of equipment and determine its value to the overall SCADA/control system and give it a value ranking (1—low value, 5—critical).

Each business unit will develop and document the criteria for assigning the value ranking to the equipment. Use the bullets below as a guideline in developing the criteria.

— Assess the piece of equipment to determine the impact it will have on the SCADA/control system if it became inoperable.

— If a single piece of equipment can affect the overall operation of the system, it is critical and should be assigned a rank of “5.” An example of this would be a SCADA server that does not have a hot backup, a spare or spare parts on hand.

— If a single piece of equipment can affect a section of the system, it should be given a rank of “4.” An example would be a PLC at a receiving station. This could shutdown one or many pipelines but, not the complete system.

— If a single piece of equipment can affect one site but long term could affect other sites, it should be given a rank of “3.” An example would be a non-essential booster PLC. The line could still run but at a reduced rate.

— If a single piece of equipment can affect one site but will not affect other sites, it should be given a rank of “2.” An example would be a water treatment PLC.

— If a single piece of equipment has no real impact, it should be given a rank of “1.” An example would be the backup HMI at a site.

B.2.1.2.2 Examine each equipment category and determine the impact that category would have on the SCADA/control system and give them a ranking (1—least impact, 5—most impact).

Each business unit will develop and document the criteria for determining the impact ranking.

There are many categories of equipment defined in the previous section. Each category is important to the operation of the system; however, some are more important than others and some are critical. Each category needs to be ranked so that the most critical systems can be addressed first. Give a ranking of “1” to the least important categories and a ranking of “5” to the most critical categories. Each business unit will need to develop the criteria for assigning the ranking.

B.2.1.2.3 Examine each equipment category and determine the overall susceptibility to a cyber attack and give it a ranking (1—low susceptibility, 5—high susceptibility).

Each business unit will develop and document the criteria for assigning the susceptibility ranking.

— Examine the category and determine the level of built-in security.

— Examine the category and determine the variability. Is it a top level device like a firewall or an end device that has several levels of security that have to be compromised to access it?

— Examine the category and determine the commonality of the tools needed to compromise the device.

— Examine the category and determine the knowledge level needed to compromise the system. Windows knowledge is wide spread; however, control systems knowledge is limited, but is readily available.

— Determine the overall susceptibility to a cyber attack of the equipment group and give it a ranking.

B.2.1.2.4 Examine the pieces of equipment and determine the overall risk to the SCADA/control system and give it an overall risk ranking (1—low risk, 5—high risk).

Each business unit will develop and document the criteria for assigning the overall risk ranking.

— Compare the above rankings for each piece of equipment and determine the overall risk.

— Give the piece of equipment a risk rank where “1” is a low overall risk and “5” is a high overall risk.

B.2.1.3 Evaluate a scenario of someone gaining full access to the SCADA/control system with complete knowledge of the system and all the tools needed to take control or change any logic in the system.

B.2.1.3.1 Identify situations where this could cause harm to people and/or the environment.

— For situations that are identified in this group, action needs to be considered. Safety devices need to be hard-wired so they can operate independently of the control system so they will function even if the control system has been compromised.

B.2.1.3.2 Identify situations where this could cause a long-term disruption of service that could impact the general public.

— For situations that are identified in this group a contingency plan needs to be developed or devices installed that would prevent the disruption of product flow to the general public.

B.2.1.3.3 Identify situations where this could cause a significant financial impact to [COMPANY].

— For situations that are identified in this group a plan needs to be developed and presented to management that would mitigate the financial impact.

B.2.1.3.4 Identify other impacts this could have.

— For items in this group, a risk assessment should be conducted to determine how likely it is to occur, its possible financial impact, its impact on operations, and the cost to implement preventive measures.

— Preventive measures should be implemented based on risk and impact.

B.2.1.3.5 Establish, where applicable, system backups and DRPs for the items identified above.

NOTE Establish a DRP that allows for rapid recovery from any emergency (including a cyber attack). System backups are an essential part of any plan and allow rapid reconstruction of the network. Routinely exercise DRPs to ensure that they work and that personnel are familiar with them. Make appropriate changes to DRPs based on lessons learned from exercises.

— The goal of the backup and DRP is to be able to recover from any cyber attack with minimum impact to operations.

— This plan should include step-by-step procedures to recover from the worst-case attack scenario. However, it should be written so that by skipping steps it could be used to recover from minor incidents.

- This plan should describe how a full scale exercise involving multiple work centers should be conducted. The full scale exercise will simulate a real world scenario of the system being compromised by a cyber attack. In addition it should describe how small scale exercises involving only the personnel that work on the SCADA/control system should be conducted to simulate multiple cyber attack scenarios. These exercises will be used to evaluate the effectiveness of the plan. The plan will need to be modified if the exercises indicate changes are required.

- This plan should specify a schedule for the frequency of full scale and small scale exercises.

B.3 Preventative Action

B.3.1 Each [COMPANY] unit will take the following steps to secure and control access to the SCADA/control systems.

B.3.1.1 Establish effective configuration management processes.

NOTE A fundamental management process needed to maintain a secure network is configuration management. Configuration management needs to cover both hardware configurations and software configurations. Changes to hardware or software can easily introduce vulnerabilities that undermine network security. Processes are required to evaluate and control any change to ensure that the network remains secure. Configuration management begins with well-tested and documented security baselines for your various systems.

B.3.1.1.1 Each business unit will establish a configuration management process that will effectively communicate changes so they can be evaluated for the possible impact they may have on the system security.

- The current management of change (MOC) process should be considered for this purpose. However, it may not be sufficient to handle all configuration changes.

B.3.1.2 Implement internal and external IDSs and establish effective incident monitoring.

NOTE To be able to effectively respond to cyber attacks, establish an intrusion detection strategy that includes alerting network administrators of malicious network activity originating from internal or external sources. IDS monitoring is essential 24 hours a day; this capability can be easily set up through a pager. Additionally, incident response procedures must be in place to allow an effective response to any attack. To complement network monitoring, enable logging on all systems and audit system logs daily to detect suspicious activity as soon as possible.

B.3.1.2.1 Each business unit will establish effective monitoring on the systems that the current configuration and technology allows.

B.3.1.3 Disconnect unnecessary connections to the SCADA network.

NOTE To ensure the highest degree of security of SCADA systems, isolate the SCADA network from other network connections to as great a degree as possible. Any connection to another network introduces security risks, particularly if the connection creates a pathway from or to the internet. Although direct connections with other networks may allow important information to be passed efficiently and conveniently, insecure connections are simply not worth the risk; isolation of the SCADA network must be a primary goal to provide needed protection. Strategies such as utilization of DMZs and data warehousing can facilitate the secure transfer of data from the SCADA network to business networks. However, they must be designed and implemented properly to avoid introduction of additional risk through improper configuration.

B.3.1.3.1 Isolate the SCADA/control system network from all other networks if it is practical.

This includes other SCADA/control networks that are on independent systems.

- Segregates the vulnerabilities of one network from those in another. Therefore, if one network is compromised, it is isolated to that network.

- Prevents a network problem on one network from affecting the other network.

— This enables positive control over the access to the SCADA/control systems.

— Limits the number of devices on the SCADA/control system network to those that are related to the SCADA/ control system.

— Limits the personnel that have access to the SCADA/control system network.

B.3.1.3.2 Disconnect all connections that are no longer in use.

B.3.1.3.3 Consider disconnecting connections that have a low benefit.

B.3.1.3.4 Disconnect connections that have a high risk and a low benefit.

B.3.1.3.5 Consider disconnecting connections that have a low risk/benefit rank.

B.3.1.4 Evaluate and strengthen the security of any remaining connections to the SCADA/control system. Establish a network protection strategy based on the principle of defense-in-depth.

NOTE 1 Conduct penetration testing or vulnerability analysis of any remaining connections to the SCADA network to evaluate the protection posture associated with these pathways. Use this information in conjunction with risk management processes to develop a robust protection strategy for any pathways to the SCADA network. Since the SCADA network is only as secure as its weakest connecting point, it is essential to implement firewalls, (IDSs, and other appropriate security measures at each point of entry. Configure firewall rules to prohibit access from and to the SCADA network, and be as specific as possible when permitting approved connections. For example, an ISO should not be granted “blanket” network access simply because there is a need for a connection to certain components of the SCADA system. Strategically place IDSs at each entry point to alert security personnel of potential breaches of network security. Organization management must understand and accept responsibility for risks associated with any connection to the SCADA network.

NOTE 2 A fundamental principle that must be part of any network protection strategy is defense-in-depth. Defense-in-depth must be considered early in the design phase of the development process, and must be an integral consideration in all technical decision-making associated with the network. Utilize technical and administrative controls to mitigate threats from identified risks to as great a degree as possible at all levels of the network. Single points of failure must be avoided, and cyber security defense must be layered to limit and contain the impact of any security incidents. Additionally, each layer must be protected against other systems at the same layer. For example, to protect against the insider threat, restrict users to access only those resources necessary to perform their job functions.

The principle of defense-in-depth is having multiple levels of security. For example a firewall at the connection point to the internet that connects to a DMZ with another firewall connects from the DMZ to your network. Then, the devices on the network require a password to access them.

There should be many security layers that a cyber attacker would have to transverse before being able to effect the system.

B.3.1.4.1 For each remaining connection that has a risk rank of > 1, the following steps should be considered.

— Evaluate alternate connection types that would be more secure.

— Determine if multiple different connections can be concentrated into a single secure connection.

— Where a serial connection is made to an outside entity, consider installing a DMZ device that would function as a slave to both entities, or some other system that would prevent the outside entity from writing data into the control system.

— Where possible, a firewall and/or ACL should be used to limit connectivity between specific devices. If a specific device needs to communicate with another device outside the SCADA/control systems network the communications should be limited to only the devices that need to communicate. All other ports and routes need to be locked down.

B.3.1.4.2 Establish strong controls over any medium that is used as a backdoor into the SCADA network.

NOTE Where backdoors or vendor connections do exist in SCADA systems, strong authentication must be implemented to ensure secure communications. Modems, wireless, and wired networks used for communications and maintenance represent a significant vulnerability to the SCADA network and remote sites. Successful “war dialing” or “war driving” attacks could allow an attacker to bypass all other controls and have direct access to the SCADA network or resources. To minimize the risk of such attacks, disable inbound access and replace it with some type of callback system.

— Backdoor connections should have been identified and been included in the risk analysis.

— Any backdoor (vendor/maintenance) connections with a benefit of < 4 should be disconnected.

— All temporary backdoor (vendor/maintenance) connections should be concentrated into a single connection. These connections need to have a minimum of username and password authentication. Advanced authentication such as a personal token such as secure ID, card swipe, or biometric such as retina scan, finger/thumb print can be used to provide an additional level of security beyond password authentication.

— Full time backdoor (vendor/maintenance) connection should have access limited by a firewall or ACLs.

B.3.1.4.3 Evaluate and secure dual-homed computers that connect to two different networks.

Dual homing a computer is a convenient way of allowing the computer to connect to two different networks; however, in situations where dual homing is used to communicate between two networks that are being segregated for security reasons it makes the computer a significant security risk. If the dual-homed computer is compromised it can compromise both networks.

If the dual-homed computer is used for redundancy on the same network or on two networks within the same system then this is not considered a security risk and is allowed.

— Dual-homed computers with connections between segregated networks will be disconnected and access to the second network will be through a firewall.

B.3.1.4.4 Lock down connections by removing or disabling unnecessary ports or routes.

— Evaluate the communications ports and routes needed to operate and support the SCADA/control system.

— Disable all unneeded ports.

— Limit the connectivity between equipment at different sites that are not related to each other, or do not need to communicate by using ACL in the routers. This will limit the access if one portion of the WAN is compromised.

B.3.1.4.5 Secure wireless connection from unauthorized interception and connection.

— Ethernet wireless connections that do not encrypt the data should have a secure tunnel between points to prevent unauthorized connection to the network by intercepting the wireless link.

B.3.1.5 Take measures to provide an additional level of security for the equipment that was identified as critical to the system.

B.3.1.5.1 Critical equipment needs to have an additional measure of security.

— Ensure critical equipment is physically or virtually isolated from other networks. Critical equipment should only be accessed from another network via a firewall or by strictly controlled router ACLs that span VLANs.

— Current complete backups of the software on critical equipment should be stored both on- and off-site.

— Offline backup equipment with the most current software should be provided for critical equipment.

B.3.1.6 Take measures to secure the devices that are connected to the SCADA/control system network. Focus on the device with the highest risk first.

B.3.1.6.1 Harden SCADA/control system network by removing or disabling unnecessary services.

NOTE SCADA control servers built on commercial or open-source operating systems can be exposed to attack through default network services. To the greatest degree possible, remove or disable unused services and network daemons to reduce the risk of direct attack. This is particularly important when SCADA networks are interconnected with other networks. Do not permit a service or feature on a SCADA network unless a thorough risk assessment of the consequences of allowing the service/feature shows that the benefits of the service/feature far outweigh the potential for vulnerability exploitation. Examples of services to remove from SCADA networks include automated meter reading/remote billing systems, email services, and internet access. An example of a feature to disable is remote maintenance. Numerous secure configuration guidelines for both commercial and open source operating systems are in the public domain, such as the National Security Agency's series of security guides. Additionally, work closely with SCADA vendors to identify secure configurations and coordinate any and all changes to operational systems to ensure that removing or disabling services does not cause downtime, interruption of service, or loss of support.

— Evaluate the HMIs and servers in the SCADA/control system and disable or remove any services or programs that are not needed in the operation or maintenance of the systems.

— Do a risk to benefit analysis of the services or programs used for maintenance to determine if they are needed or can be removed.

B.3.1.6.2 Implement the security features provided by device and system vendors.

NOTE Most older SCADA systems (most systems in use) have no security features whatsoever. SCADA system owners must insist that their system vendor implement security features in the form of product patches or upgrades. Some newer SCADA devices are shipped with basic security features, but these are usually disabled to ensure ease of installation. Analyze each SCADA device to determine whether security features are present. Additionally, factory default security settings (such as in computer network firewalls) are often set to provide maximum usability, but minimal security. Set all security features to provide the maximum level of security. Allow settings below maximum security only after a thorough risk assessment of the consequences of reducing the security level.

— Evaluate the security features (if any) of each device that is connected to the SCADA/control system to identify if the security features can be implemented without impacting the operation of the SCADA/control system. It is also important to identify if factory default password settings can be changed without impact to the system.

— Implement any device security feature or change the factory default password settings if it can be done without impacting the operation of the SCADA/control system.

— Where possible, implement domain security.

— Eliminate all possible local login accounts to the computers especially the accounts with administrator access. Enabled local accounts should be limited to the minimum required to provide operational support.

— Default administrator accounts should never be used. The username should be changed and given a password.

— All other administrative access to that computer should be controlled through domain security if the system is capable of being a member of a domain.

— If auto login is used, the account should have the minimum permissions that allow the operation of the system. In addition this account should be able to log in from only a specific work station.

— All shared folders should be evaluated for their necessity and have strict domain controls of their access.

B.3.1.6.3 If possible, unused connections should not be available for connection.

— If possible, unused ports should not be available for easy access. If only one connection is needed at a location then a crossover cable should be used to connect directly to the router.

— If there are open connections then the hub or switch should be physically secured, if possible.

— All routers should use ACLs to prevent unknown connections from accessing the WAN.

B.4 Oversight

B.4.1 Each [COMPANY] unit will setup an oversight program to ensure the SCADA/control system maintains and/or improves its level of security.

B.4.1.1 Perform technical audits of SCADA/control system devices and networks, and any other connected networks, to identify security concerns.

NOTE Technical audits of SCADA devices and networks are critical to ongoing security effectiveness. Many commercial and open-source security tools are available that allow system administrators to conduct audits of their systems/networks to identify active services, patch level, and common vulnerabilities. The use of these tools will not solve systemic problems, but will eliminate the “paths of least resistance” that an attacker could exploit. Analyze identified vulnerabilities to determine their significance, and take corrective actions as appropriate. Track corrective actions and analyze this information to identify trends. Additionally, retest systems after corrective actions have been taken to ensure that vulnerabilities where actually eliminated. Scan non-production environments actively to identify and address potential problems.

— An internal audit should be conducted to ensure that documentation created in B.1 and B.2 is current and up-to-date with any changes to the system and actions in B.3 have be diligently carried out.

— Periodically, a third-party audit should be conducted to ensure compliance with this security document.

B.4.1.2 Conduct routine self-assessments.

NOTE Robust performance evaluation processes are needed to provide organizations with feedback on the effectiveness of cyber security policy and technical implementation. A sign of a mature organization is one that is able to self-identify issues, conduct root cause analyses, and implement effective corrective actions that address individual and systemic problems. Self-assessment processes that are normally part of an effective cyber security program include routine scanning for vulnerabilities, automated auditing of the network, and self-assessments of organizational and individual performance.

— Each business unit should routinely assess their SCADA/control system for ways to improve the security of the system. This would include evaluating new technology and vendor tools.

B.5 Security Management

B.5.1 Each [COMPANY] unit will clearly define cyber security roles, responsibilities, and authorities for managers, system administrators, and users.

NOTE Organization personnel need to understand the specific expectations associated with protecting information technology resources through the definition of clear and logical roles and responsibilities. In addition, key personnel need to be given sufficient authority to carry out their assigned responsibilities. Too often, good cyber security is left up to the initiative of the individual, which usually leads to inconsistent implementations and ineffective security. Establish a cyber security organizational structure that defines roles and responsibilities and clearly identifies how cyber security issues are escalated and who is notified in an emergency.

B.5.1.1 Each unit will identify a cyber security manager for their SCADA/control system.

B.5.1.1.1 The cyber security manager will be a member of the [COMPANY] cyber security team and report to the overall [COMPANY] cyber security coordinator for all cyber security issues.

— The security manager will be the primary contact in the event of a cyber attack in another unit or within his/her unit.

— The security manager is responsible for notifying the [COMPANY] security coordinator if an intrusion is detected in their unit.

— The security manager is responsible for carrying out the correct course of action in his/her unit if an intrusion is detected in another unit.

— The security manager is responsible for identifying and mitigating the impact if another unit is forced to lock down the system because of an intrusion.

B.5.1.1.2 The cyber security manager will be responsible for working with the cyber security team to develop an action plan in the event of an intrusion in their unit or another unit.

— The plan should identify the different levels of the threat.

— The plan should identify the steps to be taken to mitigate the risk to the specific unit or another unit for each level of the threat.

— The plan should identify specific actions to be taken and the people that are assigned each action.

B.5.1.1.3 The cyber security manager will be responsible for assigning SCADA/control system administrators.

— The administrators will have the responsibility of ensuring that security policies are followed.

— The administrators will identify any security threats within their system.

— The administrators will monitor IDS and system logs for possible attacks.

— The administrators will support and monitor the people that need access.

B.5.1.1.4 The cyber security manager will work with the SCADA/control system administrators to determine the access levels of each user of the SCADA/control system.

— The access level should be the minimum level required for the person to complete their job.

— The access at any level should be limited to the equipment for which the person is directly responsible.

— The access level of each person should be documented.

— If possible, all access levels should be controlled centrally for ease of maintenance and positive control.

B.5.1.1.5 The cyber security managers from each of the business units along with the IT security managers will meet semiannually as the cyber security team.

— This team will be responsible for reviewing and updating the security plan when regulations, technology and other issues require it.

- This team will work together to ensure each business units security plan complies with the corporate cyber security plan.
- This team will work together to develop and update a unified threat notification and response plan that will coordinate all the IT systems and the SCADA/control systems during an attack.

B.5.1.2 Identify sensitive material and conduct training to minimize the likelihood that organizational personnel will inadvertently disclose sensitive information regarding SCADA system design, operations, or security controls.

NOTE Release data related to the SCADA network only on a strict, need-to-know basis, and only to persons explicitly authorized to receive such information. "Social engineering," the gathering of information about a computer or computer network via questions to naive users, is often the first step in a malicious attack on computer networks. The more information revealed about a computer or computer network, the more vulnerable the computer/network is. Never divulge data related to a SCADA network, including the names and contact information about the system operators/administrators, computer operating systems, and/or physical and logical locations of computers and network systems over telephones or to personnel unless they are explicitly authorized to receive such information. Any requests for information by unknown persons need to be sent to a central network security location for verification and fulfillment. People can be a weak link in an otherwise secure network. Conduct training and information awareness campaigns to ensure that personnel remain diligent in guarding sensitive network information, particularly their passwords.

The uniqueness of the SCADA/control system is a limitation for it to use traditional security measures; however, because of its uniqueness inside knowledge is needed to make a successful attack. Thus securing this knowledge is very important to the overall security of the system.

B.5.1.2.1 Limit distribution of the following information to only those that have a need to know and then only distribute the information that is needed. Do not provide the entire addressing schema to someone just because they need to know the addresses for their area of responsibility.

- Addressing schemes; this includes asynchronous multi-drop addresses, IP addresses and TCP ports.
- PLC register layouts.
- Configuration databases; this includes PLC/RTU, HMI, SCADA, communications servers, routers and firewalls.
- Protocol information.
- Types of communications.
- System layout schematics.
- Communication layout schematics.
- Types of SCADA equipment used.
- Any other information about the SCADA/control system.
- Security measures that are in place.

B.5.1.2.2 Keep SCADA/control systems data in a secure location.

- SCADA/control systems data should not be publicly available. This includes the general public and the general corporate populous.
- SCADA/control systems data may be useful to other business functions; however, the raw data should not be made readily available to all users. If the data are needed outside the SCADA/control system the data should be

summarized and placed in a data store that end users can access. Direct access to raw data should be limited.

— Program files and/or configuration files should be kept on a server with access control so only authorized personnel can access these files.

— Any other files or papers that contain information about the system such as addressing schemes and systems layouts should be kept in a secure location.

B.5.1.2.3 Label sensitive SCADA/control systems documents.

— SCADA/control systems documents that contain sensitive information should be labeled to indicate their sensitivity. There should be a label such as "For Official Use Only, Not for Distribution," "Confidential" or some other label that would indicate that the information is not to be freely distributed.

B.5.1.2.4 Training is important to ensure that people understand the sensitive nature of the SCADA/control system data.

— Inform people that have access to SCADA/control system data of the sensitive nature of this information.

— Inform them of why it is important that SCADA/control systems information should be handled correctly.

— Inform them that the information is not to be given out to anyone. Any request for information should be directed to the security manager.

Additional Resources

The following links provide a good starting point for additional information. As internet links do change, it is suggested that the user should start with the organizations' website for the updated version or other references.

[1] Australian government sponsored short (8 page) guide for CEOs and Boards of Directors better explaining the security risks associated with control systems,
http://www.wurldtech.com/library/pdf/SCADA%20Security%20Advice%20for%20CEO's.pdf

[2] National Infrastructure Protection Plan (NIPP) provides the coordinated approach that will used to establish national priorities, goals, and requirements, www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

[3] National Institute of Standards and Technology (NIST)—Computer Security Division Special Publications 800 series. Many standards exist that address specific security topics. For example, the most common 800 series documents include 800-53, *Federal Computer Systems*; 800-82, *Industrial Control Standards*; and 800-97 *Wireless*. http://csrc.nist.gov/publications/PubsSPs.html

[4] North American Reliability Council (NERC) list of vulnerabilities and mitigations,
http://www.esisac.com/publicdocs/Top_10_vuln_2006_16mar2006_ss.pdf

[5] U.S. Department of Energy's *21 Steps to Improve Cyber Security of SCADA Networks*, includes important steps control system owners should take, and is referenced in an earlier annex of this document,
http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf

[6] A collaborative initiative between industry and the U.S. Department of Energy, A *Roadmap to Secure Control Systems in the Energy Sector* is a common resource, http://www.controlsystemsroadmap.net/

[7] U.S. Department of Homeland Security, Control Systems Security Program website contains numerous publications on cyber security, http://www.us-cert.gov/control_systems/csdocuments.html#docs

[8] The Multi-State Information Sharing and Analysis Center, http://www.msisac.org/, has a variety of resources including specific procurement specifications for aspects of control systems, prepared by the U.S. Department of Homeland Security and Idaho National Labs, with active support of New York States' Chief Information Security Officer, http://msisac.org/scada/documents/12July07_SCADA_procurement.pdf

[9] United Kingdom Centre for Protection of National Infrastructure has created the *Process Control and SCADA Security—Good Practice Guidelines,* http://www.cpni.gov.uk/ProtectingYourAssets/scada.aspx

[10] SANS—Cyber security information and training, http://www.sans.org

[11] AGA Report 12, http://www.aga.org

[12] American Petroleum Institute, *Security Guidance for the Petroleum Industry*, Second Edition, March 2003

energy API®

2009 Publications Order Form

Effective January 1, 2009.
API Members receive a 30% discount where applicable.
The member discount does not apply to purchases made for the purpose of resale or for incorporation into commercial products, training courses, workshops, or other commercial enterprises.

Available through IHS:

Phone Orders:	1-800-854-7179	(Toll-free in the U.S. and Canada)
	303-397-7956	(Local and International)
Fax Orders:	303-397-2740	
Online Orders:	global.ihs.com	

Date: ______________________

□ **API Member** (Check if Yes)

Invoice To (□ Check here if same as "Ship To")

Name:
Title:
Company:
Department:
Address:

City: State/Province:
Zip/Postal Code: Country:
Telephone:
Fax:
Email:

Ship To (UPS will not deliver to a P.O. Box)

Name:
Title:
Company:
Department:
Address:

City: State/Province:
Zip/Postal Code: Country:
Telephone:
Fax:
Email:

Quantity	Title	SO★	Unit Price	Total
	RP 1113, Developing a Pipeline Supervisory Control Center		$82.00	
	RP 1130, Computational Pipeline Monitoring for Liquid Pipelines		$108.00	
	RP 1165, Recommended Practice for Pipeline SCADA Displays		$147.00	
	RP 1168, Pipeline Control Room Management		$80.00	
	Security Guidance for the Petroleum Industry		$185.00	

□ Payment Enclosed □ P.O. No. (Enclose Copy) ______________

□ Charge My IHS Account No. ______________

□ VISA □ MasterCard □ American Express
□ Diners Club □ Discover

Credit Card No.:

Print Name (As It Appears on Card):

Expiration Date:

Signature:

Subtotal	
Applicable Sales Tax (see below)	
Rush Shipping Fee (see below)	
Shipping and Handling (see below)	
Total (in U.S. Dollars)	

★ To be placed on Standing Order for future editions of this publication, place a check mark in the SO column and sign here:

____

Pricing and availability subject to change without notice.

Mail Orders – Payment by check or money order in U.S. dollars is required except for established accounts. State and local taxes, $10 processing fee, and 5% shipping must be added. Send mail orders to: **API Publications, IHS, 15 Inverness Way East, c/o Retail Sales, Englewood, CO 80112-5776, USA.**

Purchase Orders – Purchase orders are accepted from established accounts. Invoice will include actual freight cost, a $10 processing fee, plus state and local taxes.

Telephone Orders – If ordering by telephone, a $10 processing fee and actual freight costs will be added to the order.

Sales Tax – All U.S. purchases must include applicable state and local sales tax. Customers claiming tax-exempt status must provide IHS with a copy of their exemption certificate.

Shipping (U.S. Orders) – Orders shipped within the U.S. are sent via traceable means. Most orders are shipped the same day. Subscription updates are sent by First-Class Mail. Other options, including next-day service, air service, and fax transmission are available at additional cost. Call 1-800-854-7179 for more information.

Shipping (International Orders) – Standard international shipping is by air express courier service. Subscription updates are sent by World Mail. Normal delivery is 3-4 days from shipping date.

Rush Shipping Fee – Next Day Delivery orders charge is $20 in addition to the carrier charges. Next Day Delivery orders must be placed by 2:00 p.m. MST to ensure overnight delivery.

Returns – All returns must be pre-approved by calling the IHS Customer Service Department at 1-800-624-3974 for information and assistance. There may be a 15% restocking fee. Special order items, electronic documents, and age-dated materials are non-returnable.

THERE'S MORE WHERE THIS CAME FROM.

API provides additional resources and programs to the oil and natural gas industry which are based on API Standards. For more information, contact:

API MONOGRAM® LICENSING PROGRAM

Phone: 202-962-4791
Fax: 202-682-8070
Email: certification@api.org

API QUALITY REGISTRAR (APIQR®)

> ISO 9001 Registration
> ISO/TS 29001 Registration
> ISO 14001 Registration
> API Spec Q1® Registration

Phone: 202-962-4791
Fax: 202-682-8070
Email: certification@api.org

API PERFORATOR DESIGN REGISTRATION PROGRAM

Phone: 202-682-8490
Fax: 202-682-8070
Email: perfdesign@api.org

API TRAINING PROVIDER CERTIFICATION PROGRAM (API TPCP™)

Phone: 202-682-8490
Fax: 202-682-8070
Email: tpcp@api.org

API INDIVIDUAL CERTIFICATION PROGRAMS (ICP®)

Phone: 202-682-8064
Fax: 202-682-8348
Email: icp@api.org

API ENGINE OIL LICENSING AND CERTIFICATION SYSTEM (EOLCS)

Phone: 202-682-8516
Fax: 202-962-4739
Email: eolcs@api.org

API PETROTEAM (TRAINING, EDUCATION AND MEETINGS)

Phone: 202-682-8195
Fax: 202-682-8222
Email: petroteam@api.org

API UNIVERSITY™

Phone: 202-682-8195
Fax: 202-682-8222
Email: training@api.org

Check out the API Publications, Programs, and Services Catalog online at www.api.org.

energy API

1220 L Street, NW
Washington, DC 20005-4070
USA

202.682.8000

Additional copies are available through IHS
Phone Orders: 1-800-854-7179 (Toll-free in the U.S. and Canada)
303-397-7956 (Local and International)
Fax Orders: 303-397-2740
Online Orders: global.ihs.com

Information about API Publications, Programs and Services
is available on the web at www.api.org

Product No. D11642