Control Systems Cyber Security
Working Group

Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry

Document No.	INGAAControlSystemsCyberSecurityGuidelines
Release Date:	September 17, 2015
Version:	1.3

20 F Street NW, Suite 450
Washington DC 20001
Phone: (202) 216-5900
Fax: (202) 216-0877
Website: http://www.INGAA.org/

Proprietary Notice

ADDITIONAL NOTICE

The following information describes your rights and obligations regarding this publication.

This publication contains information pertinent to specific product(s) and/or program(s). You are authorized to use this information for the express purpose of using the product(s) and/or program(s) described herein. The following rules apply to this authorization.

All brand and product names referred to in this document are trademarks or registered trademarks of their respective companies. INGAA has obtained permission to use/reproduce information from companies whose products or information are referenced or duplicated here. If you have not purchased the actual products to which this document refers, then the information referred to here is not available/applicable to you and you should refer to your specific product information.

This publication may include technical inaccuracies or typographical errors. If you are aware of inaccuracies or errors, notify INGAA. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. INGAA may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time.

Document No.: INGAAControlSystemsCyberSecurityGuidelines

Issue Date: January 31, 2011

Revision Date: September 17, 2015

Printed in the United States of America

INGAA Proprietary Information

This document contains information that is confidential and proprietary to INGAA its affiliates, subsidiaries, suppliers, and/or third parties, and may not be disclosed except under obligations of confidentiality and subject to the provisions of a Non-Disclosure Agreement between the proposed recipient and INGAA or any of its affiliates, as applicable, or without the prior written consent of INGAA.

Revision History

Author	Change No.	Revision Date	Revision Summary
CSCSWG	0	Jan 31, 2011	Initial Release
CSCSWG	1	Jan 31, 2011	Updated References
CSCSWG	2	Mar 03, 2011	Updated References
CSCSWG	3	Sep 17, 2015	Appendix F Added

Table of Contents

Section **Page**

List of Figures

A Statement from the American Gas Association

The American Gas Association (AGA) commends the INGAA CSCSWG for its commitment to the development of a comprehensive guideline focused on cyber security of natural gas transmission process control systems. Where applicable to gas utility operations, AGA encourages the consideration of these guidelines.

1 Introduction

1.1 Background

Pursuant to the Aviation and Transportation Security Act (ATSA) (Pub L. 107071) and specific delegation by the Secretary of Homeland Security, Transportation Security Administration (TSA) acts as the lead Federal entity for transportation security, including hazardous materials and pipeline security. In 2008 TSA circulated a draft of its updated Pipeline Security Guidelines. The scope of their document encompasses all onshore transmission natural gas and hazardous liquid pipeline and liquefied natural gas operators. The TSA guidelines provide criteria which operators must use to assess and determine criticality of each of their facilities. In addition the guidelines identify baseline security risk reduction measures that must be implemented at each facility, as well as enhanced measures that must be implemented at facilities determined to be critical.

Also in their guidelines, TSA recommends that a risk-based Corporate Security Program (CSP) plan be established and employed by each pipeline industry operator to address and document the organization's security policies and procedures for managing security related threats, incidents, and responses. The CSP plan should be customized to the needs and scope of the company but at minimum must:

- Document the company's security related polices, and procedures including methodologies used and timelines for conducting criticality assessments, security vulnerability assessments (SVA), and identify baseline measures implemented at all company facilities, and enhanced measures implemented at critical facilities as outlined in the Security Measures and Cyber and SCADA System Security Measures Sections 6 and 7 of their guidelines;
- Document or reference the company's Continuity of Operation Plans (COOPs), and Incident Response and Recovery Plans;
- Be secure and protected from unauthorized access based on company policy; and
- Be reviewed on an annual basis, and updated as required based on changes or findings from the SVA, enhancements or significant changes to the system or any of its facilities or environment of which it operates.

In addition, the CSP plan including its appendices and attachments must be comprehensive in scope, systematic in its development, and risk-based reflecting the security environment.

As part of the required CSP plan operators must include a control system cyber security plans section. This section of the CSP plan must include the control system cyber security policies, practices, and procedures necessary to implement the CSP plan. Proper control system cyber security plans address, at a minimum, items of access determination and granting, server and system protection, system penetration, malicious code detection, business resumption and disaster recovery.

1.2 Purpose

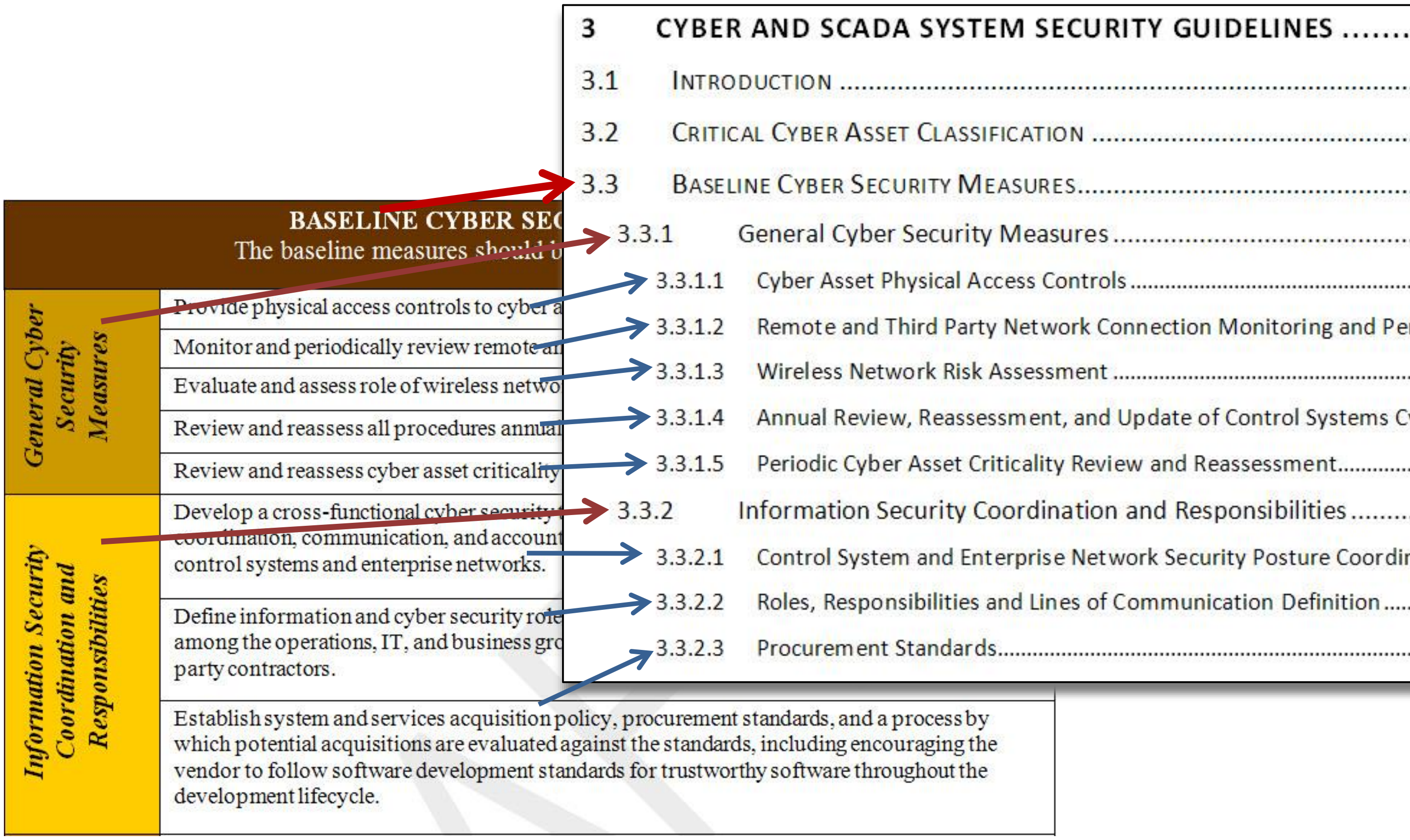
The purpose of this document is to provide guidance on addressing the control system cyber security plans section of the natural gas pipeline operators' TSA required CSP. It is a set of guidelines to assist operators of natural gas pipelines in managing their control systems cyber security requirements. It sets forth and details the unique risk and impact-based differences between the natural gas pipeline industry and the hazardous liquid pipeline and liquefied natural gas operators referenced equally in the aforementioned TSA guidelines.

1.3 How to Read These Guidelines

This document was created in response to TSA's Pipeline Security Guidelines.

Section 2 of this document provides a common basis of understanding of the natural gas pipeline industry from a cyber security perspective. Specifically, it provides an overview of the industrial control system industry in order to document its breadth and depth. It then narrows the focus to the control systems used within the interstate natural gas pipeline industry and provides an in-depth definition of its components. Lastly, Section 2 details the natural gas pipeline industry's uniqueness which differentiates it from other pipeline industries in their market, operational and security characteristics.

Section 3 of this document provides guidelines on developing Control System Cyber Security Plans as required in TSA's Pipeline Security Guidelines. TSA's guidelines implement a table structure to categorize and itemize each cyber security element of concern. As such, the format, structure, and flow of this section follows TSA's cyber security table. That is, the items in this section and their order directly follow TSA's Cyber Security table. If a TSA table entry contains multiple or compound sentences, and therefore, separate requirements, each were broken out into a unique subsection. This content and flow dependency between guidelines is depicted in the following diagram.



BASELINE CYBER SEC The baseline measures should b	
General Cyber Security Measures	Provide physical access controls to cyber a
	Monitor and periodically review remote an
	Evaluate and assess role of wireless netwo
	Review and reassess all procedures annual
	Review and reassess cyber asset criticality
Information Security Coordination and Responsibilities	Develop a cross-functional cyber security coordination, communication, and account control systems and enterprise networks.
	Define information and cyber security role among the operations, IT, and business gro party contractors.
	Establish system and services acquisition policy, procurement standards, and a process by which potential acquisitions are evaluated against the standards, including encouraging the vendor to follow software development standards for trustworthy software throughout the development lifecycle.

Figure 1: TSA Cyber Security Table to INGAA Guidelines Section 3 Item Dependency

1.3.1 Compliance Imperatives

The following terminology was strictly adhered to throughout this document. The following terms were only used to indicate the level necessity to implement an item for compliance to TSA's Pipeline Security Guidelines, or to limit behavior, which has potential for causing harm.

The key words "*MUST*", "*MUST NOT*", "*REQUIRED*", "*SHALL*", "*SHALL NOT*", "*SHOULD*", "*SHOULD NOT*", "*RECOMMENDED*", "*MAY*", and "*OPTIONAL*" in this document are to be interpreted as follows:

1.3.1.1 MUST

This word, or the terms "*REQUIRED*" or "*SHALL*", mean that the definition is an absolute requirement needed for compliance with TSA's guideline.

1.3.1.2 MUST NOT

This phrase, or the phrase "*SHALL NOT*", means that the definition is an absolute prohibition for compliance with TSA's guideline.

1.3.1.3 SHOULD

This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to not implement a particular item, but the full implications *must* be understood and carefully weighed before choosing a different course. The reason(s) for not implementing an item described with this label *must* be reasonable, defendable, and *should* be documented.

1.3.1.4 SHOULD NOT

This phrase, or the phrase "*NOT RECOMMENDED*" means that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications *should* be understood and the case carefully weighed before implementing any item described with this label. The reason(s) for not implementing an item described with this label *must* be reasonable, defendable, and *should* be documented.

1.3.1.5 MAY

This word, or the adjective "*OPTIONAL*", means that an item is truly optional. One solution may choose to include the item because a particular marketplace requires it or because the operator feels that it enhances the solution while another operator may omit the same item.

1.3.2 Application of these Imperatives

The imperatives defined above were used in this guideline with care and sparingly. For example, *must* was not used to impose a particular method on implementers where the item is not absolutely required for compliance to TSA's Pipeline Security Guidelines.

1.4 Intended Audience

The intended audience for this document is natural gas pipeline control system administrators; network security personnel responsible for securing control systems, SCADA software manufacturers for the natural gas pipeline industry, operators, TSA personnel responsible for natural gas pipeline security, vendors supplying SCADA-related products, and other governmental stakeholders.

2 Overview

INGAA is a non-profit trade association that represents the interstate natural gas transmission pipeline industry. INGAA's members operate over two thirds[1] of the nation's natural gas transmission pipeline mileage, and represent almost one quarter of the individual natural gas transmission pipeline entities reporting to PHMSA.

2.1 Industrial Control Systems

Industrial control system (ICS) is the term used to identify many types of control systems, including:

- Supervisory control and data acquisition (SCADA) systems used for oil and gas pipelines, electrical power grids, water distribution and wastewater collection systems, and railway transportation systems.
- Distributed control systems (DCS) used to control industrial processes such as electric power generation, oil and gas refineries, water and wastewater treatment, and chemical, food, and automotive production
- Local control system types include Programmable Logic Controllers (PLC) used in the critical infrastructures and the industrial sector. While PLCs are control system components used throughout SCADA and DCS systems, they are often the primary components in smaller control system configurations used to provide process control of discrete processes such as gas distribution compressor station control, automobile assembly lines, third party logistics conveyor control and power plant soot blower controls. PLCs are used extensively in almost all industrial processes.

2.2 Document Scope

The scope of this document addresses larger systems of SCADA for the natural gas transmission industry and the local control systems used throughout the pipeline system including compressor stations, production stations, M&R stations, storage facilities, and gas conditioning and dehydration stations. As such, this section provides an overview of these types of control systems, including example architectures and components.

Diagrams are presented to depict the network connections and components typically found on each system to facilitate the understanding of these systems. The diagrams in this section do not address security nor do they represent a secure architecture.

[1] INGAA members operate 223,000 miles of the 319,000 miles of natural gas transmission pipelines and 349 of the 1417 natural gas transmission operators reporting to PHMSA in 2007.

2.3 Natural Gas Transmission Control Systems

Pipelines used in the interstate natural gas transmission industry can be spread over a footprint of hundreds or even thousands of square miles/kilometers. The components, known as assets, that comprise these pipeline systems are geographically dispersed across this footprint. The Natural Gas Transmission Control fall into two types: SCADA Systems and Local Control Systems.

2.3.1 SCADA Systems

A SCADA system is highly distributed. It is specifically designed to address long-distance communication challenges such as delays and data loss posed by the various communication media in use.

A SCADA system enables the centralized supervisory control and data acquisition required for monitoring the remote assets over long-distance communications networks, including monitoring alarms and processing status data. They are critical for maximizing pipeline capacity and efficiency with the overarching requirement of safe proper operation of the pipeline.

2.3.1.1 Supervisory Control

A SCADA system enables supervisory control of the pipeline’s geographically dispersed assets. For safety reasons, the supervisory nature of a SCADA host is such that it is not allowed to override regulatory local control systems. This provides the first layer of protection for the entire control environment.

Based on information received from remote assets, automated or operator-driven supervisory commands can be pushed to remote station control devices, which are often referred to as field devices.

Field devices control local operations such as opening and closing valves, collecting data from sensor systems, and monitoring the local environment for alarm conditions. The local control system will not operate on commands sent by the SCADA host that will compromise the integrity and safety of the pipeline.

2.3.1.2 Data Acquisition

A SCADA system enables the centralized monitoring of remote assets including monitoring alarms and processing status data. It is designed to collect field information from field sites, transfer it to a central computer facility, and display the information to the pipeline operator graphically or textually, thereby allowing the operator to monitor or control an entire system from a central location in real time.

The field devices are responsible for collecting data from sensors in the form of content analysis (e.g. Octane, Nitrogen, etc), area, counts, distance, rate, factor, position, power, pressures, speed, state, temperature, time, torque, voltage, and quantities. These values are stored in the field devices to be retrieved by the SCADA host.

The field devices are also responsible for storing electronic flow measurement (EFM) data which is periodically collected by the SCADA host and forwarded to the measurement system.

2.3.1.3 Reference Architecture

A SCADA system integrates data acquisition systems with data transmission systems and Human Machine Interfaces (HMI) software to provide a centralized monitoring and control system for numerous process inputs and outputs. SCADA systems are designed to collect field information, transfer it to a central computer facility, and display the information to the operator graphically or textually, thereby allowing the operator to monitor or control an entire system from a central location in real time.

The following figure shows an example of SCADA system architecture.

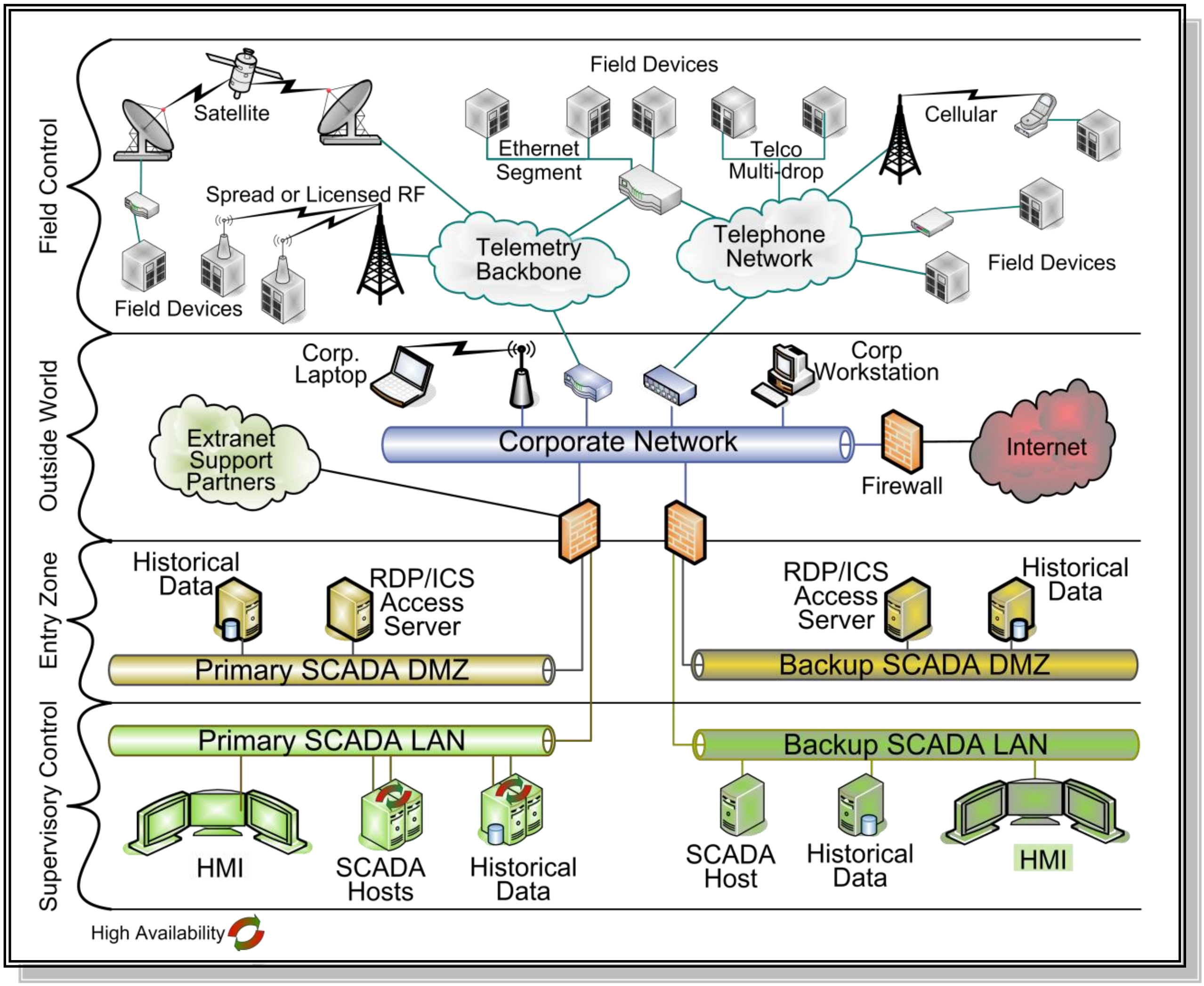


Figure 2: SCADA Reference Architecture

2.3.1.4 SCADA System Component Overview

In accordance with TSA's definition the term "system" refers to interconnected hardware and software components comprising computers, databases, applications, control and monitoring devices that together perform a particular function or interrelated set of functions. Therefore a SCADA system consists of three major components:

Centralized Monitoring and Control: SCADA Servers, HMI workstations, and Engineering workstations.

Communications Infrastructure: High bandwidth land lines; Medium bandwidth Satellites; and low bandwidth serial leased line and dial up phone lines.

Field Site devices and equipments: RTU, PLC, and or flow computers which control actuators and/or monitors sensors. The field devices control the local process.

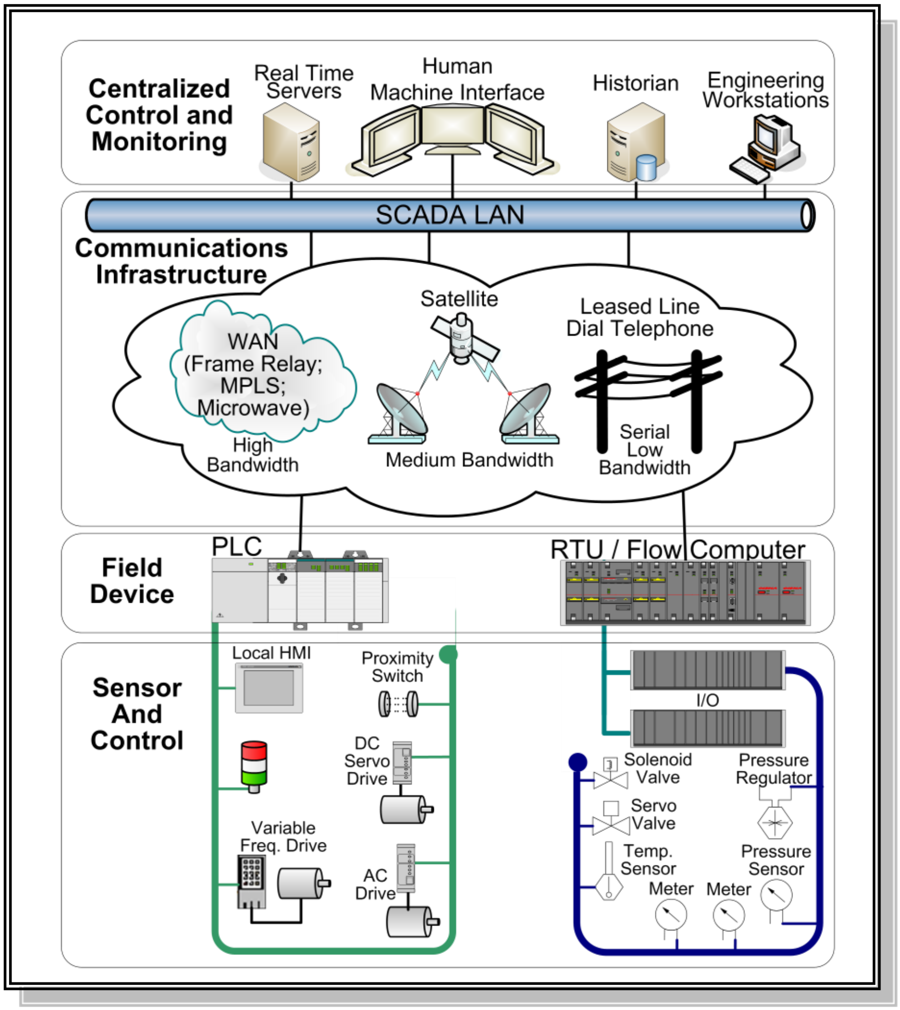


Figure 3: SCADA System Components Overview

2.3.1.5 SCADA System Component Hierarchy

The centralized monitoring and control architecture of a SCADA system dictates a hierarchical relationship between the host system and the communications infrastructure and field sites in its domain.

There is a single host that communicates over multiple communication channels within the communication infrastructure. Each communication channel within the communication infrastructure can have multiple field devices connected. Each field device can then in turn have multiple input sensors and output controls in its domain. This is depicted in the following diagram.

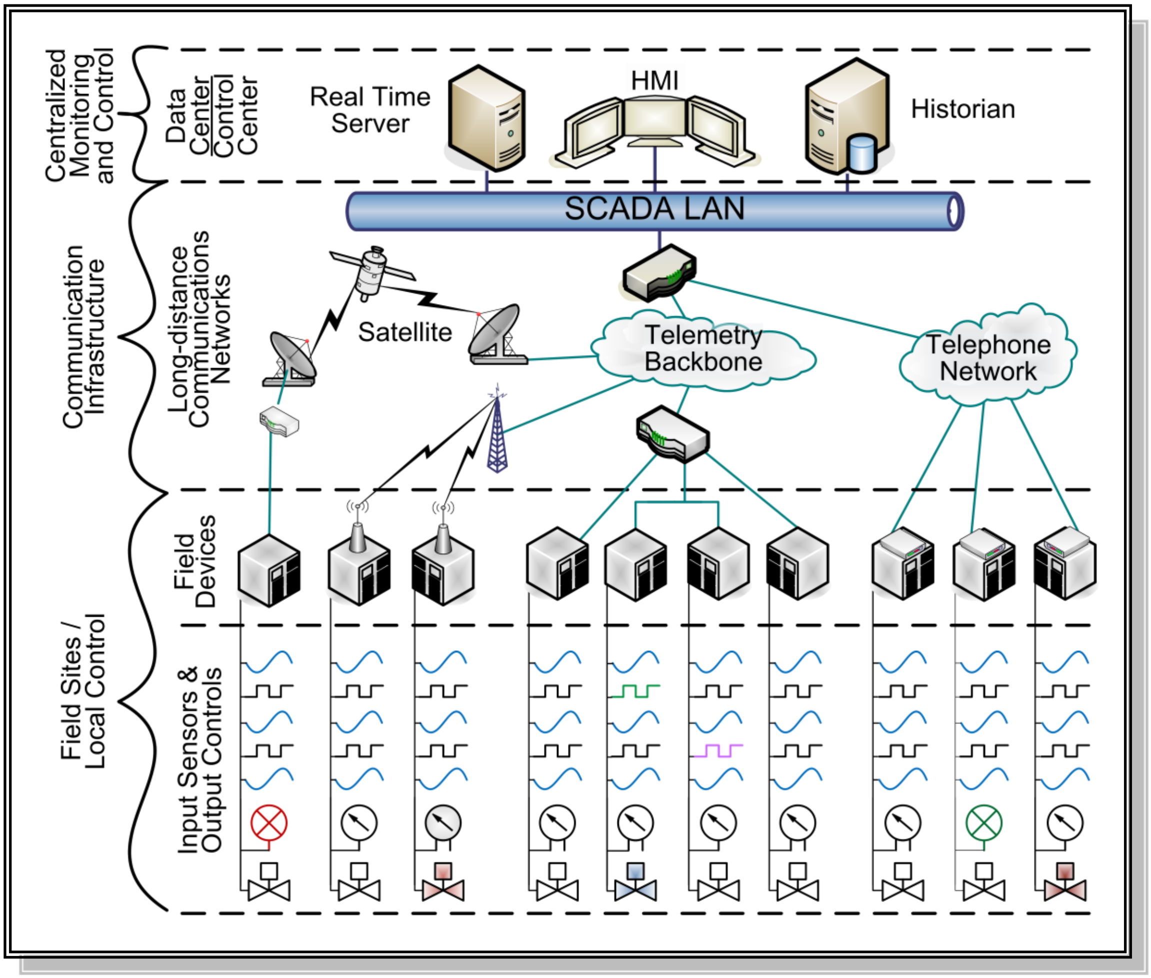

Centralized Monitoring and Control
Data Center Control Center
Real Time Server
HMI
Historian
SCADA LAN
Communication Infrastructure
Long-distance Communications Networks
Satellite
Telemetry Backbone
Telephone Network
Field Sites / Local Control
Field Devices
Input Sensors & Output Controls

Figure 4: Centralized Monitoring and Control SCADA System Components Hierarchy

To provide clarity of definition and minimize confusion and misinterpretation, the following sections define the key SCADA System components that are used in monitoring, control and networking.

2.3.1.6 Centralized Monitoring and Control Environments

- **SCADA System:** Refers to the entire system: all SCADA servers, Human Machine Interface workstations, and Communications equipment and infrastructure.
- **Primary Data Center:** The Primary Data Center houses the SCADA hosts and some of the communications infrastructure.
- **Backup Data Center:** The secondary data center houses a complete secondary set of SCADA hosts and some backup communications infrastructure. It is put in place to provide high availability of the SCADA system.
- **Primary Control Center:** The Primary Gas Pipeline Control Center is the main centralized facility used to control the pipeline. It is occupied on a continuous basis using rotating shifts of pipeline operators.
- **Backup Control Center:** The Backup Gas Pipeline Control Center is the alternate centralized facility used to control the pipeline when the Primary Control Center is unavailable. It is usually located in a separate distinct geographic location from the Primary Control Center to mitigate the pipeline operations impact when the Primary Control Center is unsafe or unavailable for occupancy. When in use, the Backup Control Center is occupied on a continuous basis using rotating shifts of pipeline operators until the Primary Control Center is safe and available to be reoccupied.
- **Interim Control Center:** The Interim Control Center is implemented as a stop-gap or short term use control center. This location is usually within the same metropolitan area for quick and easy access. It is occupied for short durations while the Primary Control Center is unavailable. It can be occupied during the transition from the Primary Control Center to the Backup Control Center.
- **SCADA Servers:** The SCADA Server is the device that acts as the master in a SCADA system. Remote terminal units and PLC devices (as described below) located at remote field sites usually act as slaves.
- **Human-Machine Interface (HMI):** The HMI is software and hardware that allows human operators to monitor the state of a process under control, modify control settings to change the control objective, and manually override automatic control operations in the event of an emergency. The location, platform, and interface may vary greatly. For example, an HMI could be a dedicated platform in the control center, a laptop on a wireless LAN, or a browser on any system connected to the Internet.
- **Historian:** The data historian is a centralized database for logging all process information within an ICS. Information stored in this database can be accessed to support various analyses, from statistical process control to enterprise level planning.
- **Input/Output (IO) Server/Gateway:** The I/O server or I/O Gateway is a control component responsible for collecting, buffering and providing access to process information from control sub-components such as PLCs, RTUs and Smart Sensors. This device can reside on the control server or on a separate computer platform. They are also used for interfacing with third-party control components, such as an HMI and a control server.

2.3.1.7 Communications Infrastructure Components

There are different network characteristics for each layer within a control system hierarchy. Network topologies across different ICS implementations vary with modern systems using Internet-based IT and enterprise integration strategies. Control networks have merged with corporate networks to allow engineers to monitor and control systems from outside of the control system network. The connection may also allow enterprise-level decision-makers to obtain access to process data. The following is a list of the major components of an ICS network, regardless of the network topologies in use:

- **SCADA LAN:** Local Area Network that connects all SCADA servers within a Data Center. Often the SCADA LAN can include both the Primary SCADA LAN and the Backup SCADA LAN.
- **Primary SCADA LAN:** Local Area Network within the Primary Data Center used to interconnect the SCADA servers.
- **Shared WAN Infrastructure:** Wide Area Network communication infrastructure used by both the SCADA system and the business users and applications.
- **Routers:** A router is a communications device that transfers messages between two networks. Common uses for routers include connecting a LAN to a WAN and connecting SCADA server and RTUs to a shared WAN infrastructure for SCADA communication.
- **Firewall:** A firewall protects devices on a network by monitoring and controlling communication packets using predefined filtering policies. Firewalls are also useful in managing ICS network segregation strategies.
- **Modems:** A modem is a device used to convert between serial digital data and a signal suitable for transmission over a telephone line to allow devices to communicate. They are also used in both SCADA systems, DCSs and PLCs for gaining remote access for operational functions such as entering command or modifying parameters, as well as for diagnostic purposes. Modems are often used in SCADA systems to enable long-distance serial communications between SCADA server and remote field devices.
- **Remote Access Points:** Remote access points are distinct devices, areas and locations of a control network for remotely configuring control systems and accessing process data. Examples include using a personal digital assistant (PDA) to access data over a LAN through a wireless access point, and using a laptop and modem connection to access an ICS system remotely.
- **Control Network.** The control network connects the supervisory control level to lower-level control modules.
- **Field Network.** The field network links field devices (PLC/RTU) to other field devices and links sensors and other devices to a PLC or other controller. The sensors communicate with the field controller using a specific protocol. The messages sent between the sensors and the controller uniquely identify each of the sensors.

2.3.2 Field Systems

Field systems can be broken down into two categories, each having one or more safety related features: Local Control Systems and Local Safety Systems.

2.3.2.1 Local Control System Component Overview

The components of a local control system consist of the following:

- **Remote Terminal Unit (RTU):** The RTU, also called a remote telemetry unit, is special purpose data acquisition and control unit designed to support SCADA remote stations. RTUs are field devices often equipped with wireless radio interfaces to support remote situations where wire-based communications are unavailable.
- **Programmable Logic Controller (PLC)**: The PLC is a small industrial computer originally designed to perform the logic functions executed by electrical hardware (relays, drum switches, and mechanical timer/counters). PLCs have evolved into controllers capable of controlling very complex processes. They are used substantially in SCADA systems and DCSs. In SCADA environments, PLCs are replacing special-purpose RTUs as field devices because they are more economical, versatile, flexible, and configurable.
- **Flow Computer:** A flow computer is an electronic device which implements algorithms to turn raw data received from flow meters to which it is connected into volumes at base conditions. It also audits changes that have been made to any of the parameters required to turn the raw flow meter data into volumes. It records events and alarms related to the flow meter. It will keep a running tally of the volume for each flow meter it monitors and perform a gauge off of this volume on an hourly, daily or monthly basis. The flow data is made available externally through an electronic interface so that a SCADA system can obtain the information for the purposes of supervision, accounting or auditing.
- **Smart Sensors:** Sensors/actuators contain the intelligence required to acquire data, communicate to other devices, and perform local processing and control. A Smart Sensor could combine an analog input sensor, analog output, low-level control capabilities, a communication system, and program memory in one device.

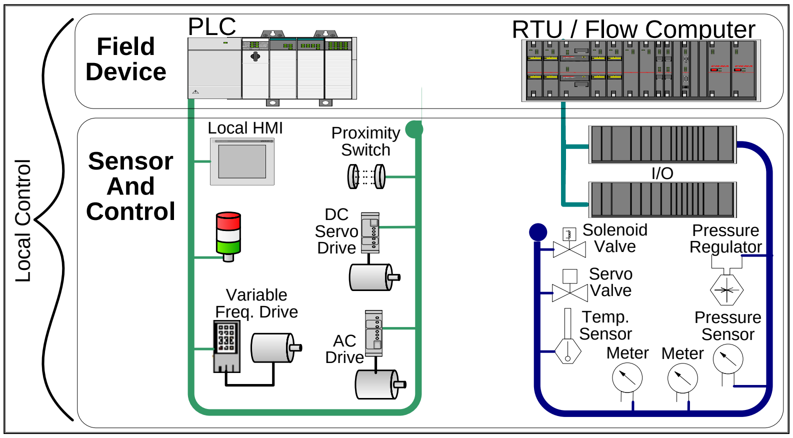


Figure 5: Local Control System Components

2.3.2.2 Local Control System Safety

The local control system components mentioned above provide one of the layers of protection for the entire control environment. They are integrated to provide a common control environment to monitor and control the facilities within their safety-related operating parameters. These parameters are provided by the engineering specifications of the facility as required by government regulations.

Significant facilities, including but not limited to compressor, storage, dehydration, and meter facilities, have specific logic and controls designed and installed to ensure the safe operation of the facility. For example, some facilities contain valves operated by the local control system to manage flow when a safety situation arises.

2.3.2.3 Local Safety Systems

Larger facilities may contain emergency shutdown systems (ESD) that run independently from their control systems. The ESD system detects fire, hazardous gas, manual pushbuttons, and primary control system malfunction to return the facility to a safe state in the event of adverse operating conditions. Also, non-ESD related facility conditions are monitored for safe operation like low oil pressure, high jacket water temperature, engine over-speed, surge conditions and high discharge pressure.

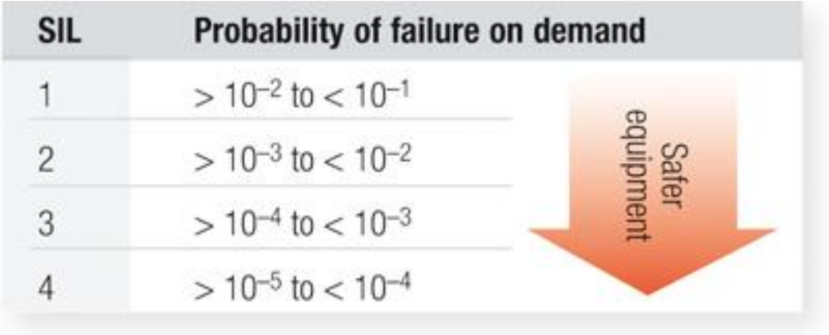
Smaller facilities may also have secondary safety systems. As a common practice, meter facilities that contain a flow control valve have secondary safety systems that are independent of the EFM system.

Process Safety Management (PSM) is an analytical tool focused on preventing release of any substance defined as a “Highly Hazardous Chemicals” by the EPA or OSHA. Any facility that stores or uses a defined “highly hazardous chemical” must comply with OSHA’s PSM regulations Title 29 CFR 1910.119. For PSM facilities, the design process strives for safe operation through mechanical mitigation of identified risks. The process used to identify and address the risks to the safe operation of a PSM facility starts with a process hazard analysis which is then used to do a Layer of Protection Analysis (LOPA). As part of the LOPA, a Safety Integrity Level (SIL) is associated with each risk and an appropriate solution based on the SIL outcome. SIL is a measurement of performance required for a Safety Instrumented Function (SIF). It is a relative level of risk-reduction provided by a safety function. A SIL is determined based on a number of quantitative factors in combination with qualitative factors such as development process and safety life cycle management.

The SIL requirements for hardware safety integrity are based on a probabilistic analysis of the device. To achieve a given SIL, the device must have less than the specified probability of dangerous failure and have greater than the specified safe failure fraction.

The SIL requirements for systematic safety integrity define a set of techniques and measures required to prevent systematic failures (bugs) from being designed into the device or system. These requirements can either be met by establishing a rigorous development process, or by establishing that the device has sufficient operating history to argue that it has been proven in use.

Four SILs are defined, with SIL4 being the most dependable and SIL1 being the least. The figure below shows the SIL:



SIL	Probability of failure on demand
1	$> 10^{-2}$ to $< 10^{-1}$
2	$> 10^{-3}$ to $< 10^{-2}$
3	$> 10^{-4}$ to $< 10^{-3}$
4	$> 10^{-5}$ to $< 10^{-4}$

Safer equipment

Figure 6: Local Control System Safety Integrity Levels

The Safety Instrumented System (SIS) is then designed with a desirable mechanical mitigation solution to meet the requirements of the target SIL. Should a mechanical system be unavailable or deemed insufficient, an active control system can be used to actively monitor and control the risk mitigation process.

As a result, SIS and/or ESD systems monitor the compressor station equipment independent of the local control and the supervisory control (i.e. SCADA system) to ensure safe operations within a tolerable level of risk.

2.4 Natural Gas Transmission Pipeline Unique Characteristics

2.4.1 Market and Operational Characteristics

Natural gas supplies over 25% of the nation's residential, commercial, industrial, and transportation energy needs. Being a gaseous product, the only feasible way to transport this product a long distance is through transmission pipelines. Natural gas is considered to be a fungible and interchangeable product allowing tremendous flexibility in delivering the product to the customer.

The most significant distinguishing trait of natural gas transmission pipelines is the physical characteristics of the product being transported. The first characteristic of natural gas[2] is that it is lighter than air. Any escaped natural gas expands, rises and then quickly dissipates. This makes venting and the subsequent dissipation of natural gas to the atmosphere a safe, acceptable option at many locations in the event of an emergency. Secondly, as a compressible fluid, natural gas is transported by pressurizing the gas, injecting the gas into a pipeline where it flows through the pipeline with a corresponding drop in pressure over distance traveled. This characteristic results in a certain amount of high pressure "pack gas" that is in the pipeline system at all times. This pack gas continues to provide gas to lower pressure delivery locations for some period of time without compression or additional natural gas being introduced into the pipeline system.

A depiction of the natural gas value chain is shown below within the circled section. These natural gas transmission pipelines provide the infrastructure to transport natural gas which is owned by the shippers (business model similar to the internet network providers). There are approximately 200,000 miles of these interstate natural gas transmission pipelines.

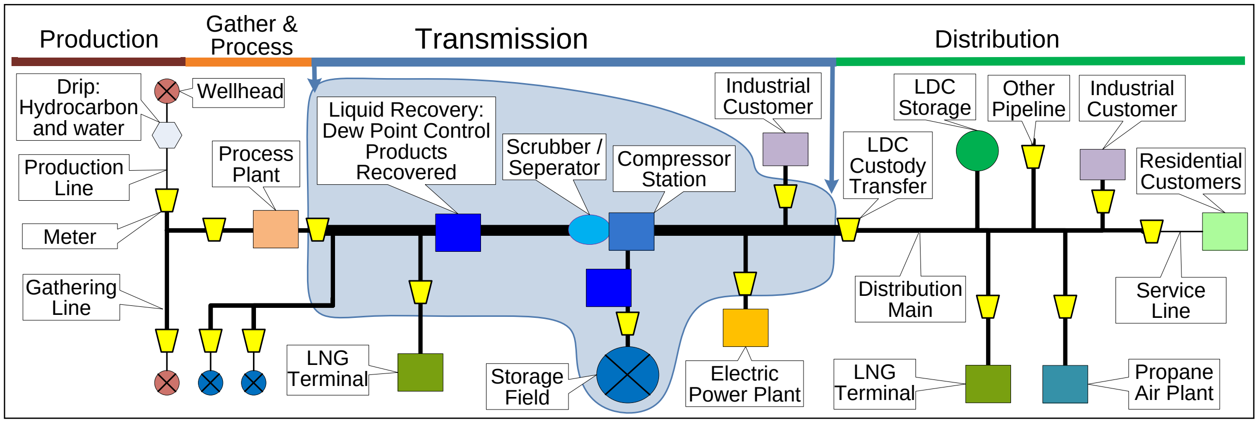
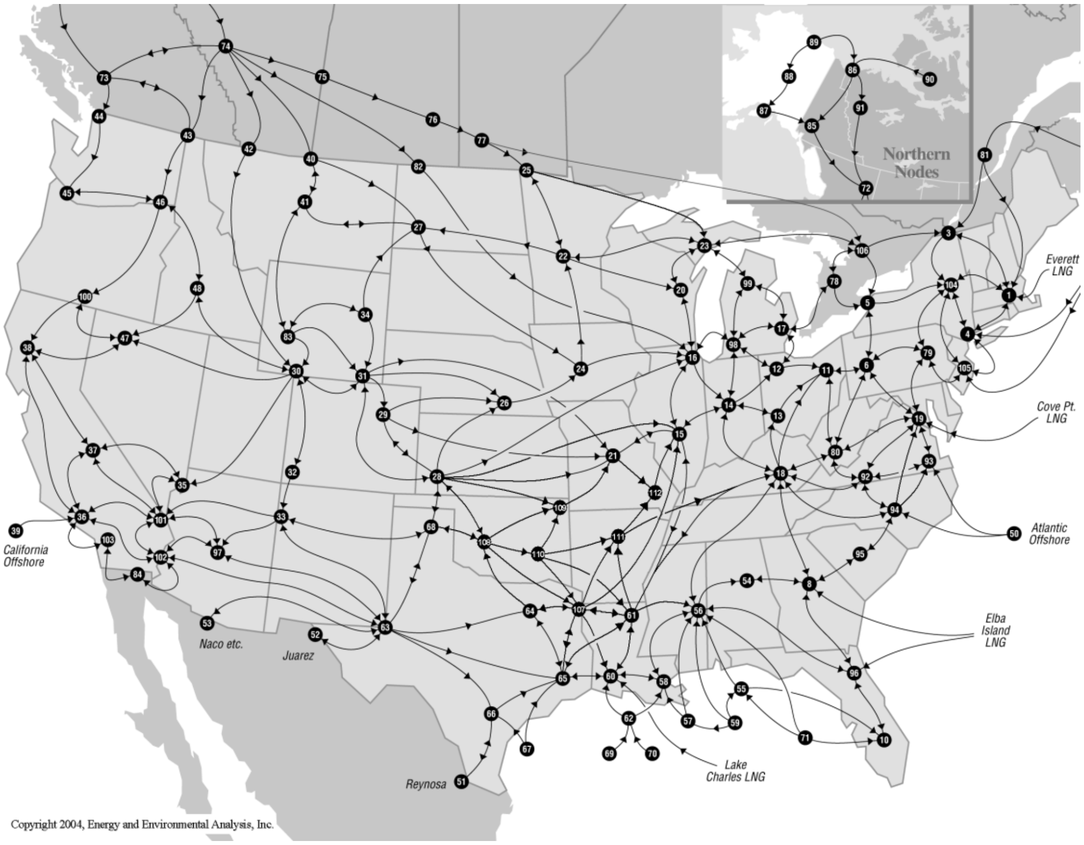


Figure 7: Pipeline Physical Characteristics

The interstate natural gas transmission pipeline system within North America can be described as a nodal network in which natural gas enters (supply) and exits (demand) the nodal network at various points. A simplified diagram of this network is shown below.

[2] Natural gas is primarily composed of methane.



Copyright 2004, Energy and Environmental Analysis, Inc.

The motive force to transport the natural gas within the network as well as manage the inventory of the product within the nodal system is through the asynchronous management of the operating pressure of the natural gas (by distributed compressor stations) within segments the pipeline network. To further manage inventory of the product, there are specific locations within the nodal system that permit natural gas to accumulate and deplete in underground storage facilities to help manage the disparity between supply and demand. In some instances the physical pipeline capacity itself can also be leveraged to meet short term gas delivery demand. This is accomplished by essentially storing gas in the pipeline at high pressure during a period of low demand and then allowing the pressure to decrease and drawn down the gas during a period of high demand. This approach is usually used to manage daily fluctuations in gas delivery demand whereas underground storage facilities are usually utilized to manage seasonal fluctuations in gas delivery demand. The product transported in this network, compressed natural gas, physically moves within this network at an average velocity of 15mph, resulting in a very high inventory/ demand ratio that is widely distributed throughout the nation. As an interchangeable product, only the total gas into and out of the pipeline system requires measurement and individual units or batches of gas are not tracked.

This integrated design permits flexibility of interchanging the delivered commodity, multiple flow paths for the natural gas to reach markets, the ability to buffer changes in supply and demand, the ability to handle quick transient flow conditions, and a singular primary control variable[3], pressure of the natural gas. The result is an inherently resilient transportation

[3] For example, electricity has two control variables; frequency and voltage.

and inventory design, no matter how the control of the system is managed. More information can be obtained on the operations of interstate natural gas pipelines by reviewing INGAA's Interstate Natural Gas Pipeline Efficiency, published in October 2010.

2.4.2 Security Characteristics

An interstate natural gas transportation system typically consists of a large number of above-ground small footprint physical facilities and extensive below-ground pipeline segments. The above-ground and below-ground pipeline segments[4] for a given pipeline system are usually located over a wide geographic area. Gas enters the pipeline systems at numerous above ground measurement facilities and is transported via pipelines to numerous above ground measurement facility where the gas exits a given pipeline system. Natural gas is compressed to relatively high pressures before it is introduced into the pipeline system (receipt point) and at intervals along the pipeline (compressor stations).

The above ground physical facilities principally consist of gas measurement facilities and compressor stations. Gas measurement facilities are defined as facilities that measure the gas that enters and exits the pipeline system. These measurement facilities are designed to prevent overpressure of the pipeline system in emergency situations by the use of mechanically controlled devices that prevents overpressure or provides a controlled release of the natural gas to atmosphere. Gas compression stations compress the gas for transportation in a pipeline segment. Emergency mechanical control devices are also employed at these compression facilities to prevent overpressure of the piping system by shutting down compressors or providing a controlled release of the natural gas to atmosphere.

ICSs are used to provide both supervisory control and data acquisition (SCADA) capabilities for entire pipeline systems and local control and data acquisition at a particular facility. The design and use of ICS in the natural gas transportation industry is somewhat unique due to the physical characteristics of natural gas and the nature of the physical facilities as compared to other energy transportation systems.

The above ground physical facilities associated with a natural gas transportation system are both widely distributed geographically and often located in remote areas. This has led the industry to adopt a practice of designing each facility so that it is safety independent. The safety devices that protect the physical assets and public safety are independent of both the SCADA system and any local ICS system. In addition the local ICS systems are designed to continue operation independent of the centralized SCADA system. This means that the local compressor station control system or the local gas measurement system will continue to perform all essential functions without the supervisory control system.

These aforementioned characteristics have an impact upon the design of ICS security. First, not all facilities are critical, which leads to a risk base approach to security. Thus, a wide range of cyber security measures are available and appropriate at different facilities depending upon the risk associated with a particular facility.

[4] Average depth of pipeline is three feet.

Secondly, consistent, periodic communication between the supervisory control system and the remote facilities is not critical or even necessary for many facilities and a risk-based approach can be applied. Since each facility is inherently safe and can operate independent of the supervisory control system, neither public safety nor overall deliverability is dependent upon uninterrupted communication between the supervisory control system and the remote facilities.

2.4.3 Control System: Threats, Vulnerabilities, and Consequences

The following section describes the risk to control systems in the Natural Gas Pipeline industry. Control systems are dependent upon computers, software, and often connected to networks, which have inherent risk. Risk can be defined as the following equation: Risk = Threat X Vulnerabilities X Consequences.

- Threat: Any person, circumstance or event with the potential to cause loss or damage.
- Vulnerability: Any weakness that can be exploited by an adversary or through accident.
- Consequence: Amount of loss or damage that can be expected from a successful attack.

As such, control systems *must* be protected.

2.4.3.1 Threats

The threats to energy industry systems have expanded beyond the typical physical attacks of the past. When these physical attacks are combined with attacks on the control systems the results could be much more damaging. The changing nature of control systems mean that attackers ranging from crackers to sophisticated insiders can have physical effects through cyber means.

The new networked control systems are vulnerable to attacks that are not specifically aimed at them. The control system may not be the target but it can be affected because of its dependence on modern operating systems and networks.

New threats come from terrorists who want to destabilize energy industry supply capabilities and the national economy. The younger generation of terrorists seems to be more cyber-security oriented.

The result is that the threat horizon for control systems is widening.

2.4.3.2 Vulnerabilities

SCADA systems are now less physically isolated from the enterprise network and are therefore more vulnerable than in the past. Access to enterprise network segments is oftentimes required to meet the operators' business requirements, and access to the SCADA domain is sometimes required for support. Common IT solutions are being applied to the SCADA arena, including standard workstations and servers, operating systems, network components.

2.4.3.2.1 SCADA Integration

At one time, SCADA systems were completely isolated. However, they are increasingly being integrated into corporate networks. This growing interconnection exposes these systems to forms of attack and exploitation that previously were impossible. This can increase the exposure to attack.

2.4.3.2.2 SCADA Standardization

Paradoxically, these older isolated systems had their own inherent protection due to their unique components and protocols. Previously, these systems did not use standard components and protocols and were not susceptible to the same kind of generic attack as are newer systems. As many of these were one-of-a-kind systems, any attempt to exploit them required developing considerable knowledge which was not easily available.

Newer SCADA systems increasingly are designed around open standards and protocols and are implemented with common hardware and operating systems.

This transformation of the control system architecture is another source of vulnerability. Control systems today are retiring their traditional proprietary architectures, networks, and tools and implementing new systems based on open standards. These are being implemented in all facets of the control systems environment. TCP/IP is used for networks; Windows, Linux, and UNIX are used for operating systems; and web browsers and XML are used for information access and sharing. These standard tools increase vulnerability by exposing the control system technologies to the bright light of public domain knowledge. Security by obscurity is no longer available.

These components are popular because they are widely available, as the development costs are spread among millions of users. A disadvantage is that any vulnerability such as design flaws or backdoors is shared as well.

If a successful exploit is developed against a common component, it is likely to work against most or all the systems using that component until it is mitigated.

This exploit/fix cycle locks users of these systems into a reactive stance. The result of this standardization is that a large number of attackers focus on common systems with known vulnerabilities. As SCADA systems are increasingly based on these standard systems they become natural targets of attacks.

2.4.3.2.3 Increased System and Integration Complexity

Proprietary solutions increasingly give way to open solutions. Vendors of proprietary solutions meld their offerings into open solutions. Standardization has opened the door for increased integration. Integration of product offerings becomes an increasingly complex task.

Modern SCADA systems, integrated with business networks, increasingly make use of network infrastructure and network services, often including security and protection offerings.

Modern SCADA systems are increasingly making use of network infrastructure and network services, often including security and protection offerings as its data is integrated with business systems. Properly managing these systems and integrating them optimally is difficult.

The promise of using network services by the SCADA system is in offloading the administrative burden and maintenance from the SCADA system and staff and placing it on specialists who manage this function for the entire enterprise.

The downside is that a malfunctioning network service can impair the SCADA system as well as other less critical systems. For example an incorrectly configured switch or DNS or UPS can easily impair a SCADA system.

SCADA has traditionally been held to a very high service level commitment. If the supporting services the SCADA system depends on does not have the same or higher service level, the SCADA system service level is degraded.

Cyber events have increased dramatically since the 9/11 attack. Information Technology policies regarding internal network security as well as security regarding access to the internet have become standard practice. These policies are often written for common business networks where homogeneous Information Technology (IT) equipment is utilized. IT organizations strive for ubiquity and uniformity to lower the cost of maintenance and ownership.

Any problems with shared network services or infrastructure can now impact SCADA. A very minor or obscure change or malfunction could impair the SCADA system.

2.4.3.2.4 More Data Flow - Business Side

SCADA systems collect operational information from field locations and display this information for operations and can execute controls at select field locations.

Increasingly they are also the collectors and possibly the repository for large amounts of detailed operational and measurement history. This results in increasing numbers of data requests being made to the SCADA system.

Historically control system data was used only by the control system personnel. Control system data is now becoming a commodity often like the physical product it represents. Everybody wants data out of the control systems: from Government agencies for compliance, to partners, suppliers, engineers, business managers, maintenance personnel, and other computer applications. All of this demand for data increases the need for more integration, puts more pressure on control system staff - which is often already overloaded - to service these data requests, and diverts their attention from monitoring for potential breaches.

The integration of domains within a natural gas pipeline enterprise along with the transformation to standardization has fueled the explosion of consumers of control system data. The result is as more functions are added to the SCADA system and more data flows from it, the system becomes less robust.

The more interfaces a system has, the more attack vectors that exist.

2.4.3.2.5 More Data Flow - Process Side

Over the past ten years most enterprise organizations have migrated from proprietary communication methodologies to network based solutions for business applications. Industrial devices such as Flow Computers and PLCs have also migrated to network based solutions which provide greater access speed and increased functionality such as remote configuration and remote diagnostics.

Remote configuration of Industrial devices offers great convenience and savings. It also could be a path for exploitation.

The increasing use of digital technology is a major source of vulnerabilities. This comes in the form of ever increasing amount of data. This flood of information can overwhelm an organization and its processes.

As the devices grow in intelligence and complexity there can be increasing risk of exploitation of its expanding feature set.

2.4.3.2.6 Network Integration / Segregation

The cost of duplicate networks typically has discouraged the implementation of segregated networks for both business and control systems. Today it can be found that these field industrial devices are comingled on a common network segment with Information Technology equipment and workstations supporting the business as well as industrial controls. This type of installation can allow network access to the industrial devices from anywhere on the network.

As corporate networks evolve and extend throughout the company, SCADA circuits and traffic often ride on the corporate networks and infrastructure. Isolation and partitioning of this traffic is complex to arrange and support. Once commingled, there exists the possibility of monitoring and interfering with this traffic.

2.4.3.2.7 Extended Lifecycle

The rules and tools used to protect these homogeneous IT devices do not interact well with real time industrial devices. In most cases the industrial devices are integrated into a closely knit local network to provide systematic deterministic local control of a compressor or turbine. The combination of the components that comprise these systems are tested and certified at the time of installation. In many cases, the components that make up the certified system cannot be modified or patched without recertification.

Components that comprise these control systems typically have an expected useful life of more than 15 years which equates to over four times the life of the standard business IT workstation. The life span of the systems' software often exists well beyond the support provided by the vendor exposing vulnerabilities that were probably unknown at the time of implementation. These vulnerabilities also exist between systems of varied vintages.

Similar to the homogeneous IT equipment, vulnerabilities also exist for industrial controls equipment. By virtue of the certification process, they are not easily patched and virus protection software *may not* be used due to the critical nature of their purpose.

Older systems tend to be limited to older software. The exploits for these older systems are well known and protection *may not* exist or if it exists, it may interfere with proper operation of the system.

2.4.3.2.8 Incorporation of New Technology

Standardization in the control system environment also enables the ability to be more agile, which in turn provides the opportunity to implement new technologies before all of the security risks can be identified and understood, much less addressed. Using wireless IP enabled networks within a control network is an example of this type of technology that has infiltrated the control system without proper assessment or mitigating controls implemented. This rush to technology adds one of the most dangerous types of risk to the control system: Blind risk.

Also, the outdated mentality of assuming that the control system is in isolation increases risk.

If an organization's control systems' staff is not working diligently and consistently to improve its security posture, it is, in effect, moving backwards.

2.4.3.3 Consequences

The primary function of a SCADA system is to gather and present data to allow operators to monitor and operate the pipeline. The SCADA system is also able to exert some controls at compressor stations and other places, removing the need for local personnel to attend to these tasks.

If the SCADA system becomes impaired, some of the information will not be available and the operators will be forced to operate with a less accurate picture of the pipeline's state. However, immediate consequences will be minimal, since the remotely operated facilities are designed to maintain their normal mode of operation, independent of the SCADA system. Should the operators experience a protracted loss of information or ability to exert controls remotely, there is an increased risk that changes required to maintain efficient operation of the pipeline will not occur. As operating conditions change, the configuration of pipeline facilities may no longer be efficient, and this may eventually affect overall deliverability.

Therefore if an outage occurs and persists, the operator will respond by having critical sites monitored and controlled by local personnel.

These aforementioned characteristics have an impact upon the design of control system security. First, not all facilities are critical, which leads to a risk based approach to security. Thus, a wide range of cyber security measures are available and appropriate at different facilities depending upon the risk associated with a particular facility.

Secondly, consistent, periodic communication between the supervisory control system and the remote facilities is not critical or even necessary for many facilities and a risk-based approach can be applied. Since each facility is inherently safe and can operate independent of the supervisory control system, neither public safety nor overall deliverability is dependent upon uninterrupted communication between the supervisory control system and the remote facilities.

There can be two consequences when a natural gas transportation system is compromised to an extent where supervisory control, local control and safety control are ineffectual.

The first is if there is a rupture of the piping either due to damage or overpressure and natural gas is released. Fortunately, the behavior of released natural gas from a high pressure transmission pipeline is very well understood and in a worst case situation, only affects a small area directly around rupture site. As such, the public safety impact is limited to a local concern.

The second consequence is if there is an interruption of the delivery of natural gas to a particular market area. As mentioned before, the redundancy of the pipeline delivery system results in the ability to redirect deliveries. In addition, the simplicity and compatibility of many of the pipeline components and their construction allows for quick repairs.

3 Control System Cyber Security Plans Guidelines

3.1 Introduction

As defined earlier in this document, the term control system(s) refers to SCADA and local control systems used in the natural gas pipeline transmission industry. When the term SCADA is used it refers to SCADA systems only and not local control systems. The converse is also true; when the term local control system is used it is distinguishing the system from the SCADA system that may or may not communicate with it.

The growing convergence of information technology and control systems brings with it increased capabilities but also increased exposure to cyber attacks against infrastructure. Developing and implementing security controls reduces the risk to control systems.

As such, the operator *must* develop and implement a security plan for its control systems. This control system security plan, referred to as the control system cyber security plan, is a required section of TSA's mandated CSP. This plan *must* provide an overview of the security requirements for the operator's control systems and a description of the security measures in place or planned for meeting those requirements. It *must* also include the policies, practices, and procedures necessary to implement the CSP plan. The control system cyber security plans *should* consist of:

- Security planning policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- Procedures to facilitate the implementation of the security planning policy and associated security planning controls.

The control system cyber security plans must, at a minimum, address: access determination and granting, server and system protection, system penetration, malicious code detection, business resumption and disaster recovery.

The control system cyber security plan is aligned with the organization's control system architecture and information security architecture. To properly develop the control system security plan, it is essential for a cross-functional cyber security team to share their varied domain knowledge and experience to evaluate and mitigate risk in the control system. The cyber security team considers control system safety and security interdependencies. The cyber security team *should* include members of the organization's IT staff, control system engineers, control system operators, members with network and system security expertise, members of the management staff, and members of the physical security department. In some organizations, it *may* be necessary for personnel to perform multiple roles. For continuity and completeness, the cyber security team *must* consult with the control system vendor(s) as well.

Designated officials within the organization review and approve the control system security plan.

This section provides guidance in the creation and content of the control system cyber security section of the CSP.

The CSP control system cyber security plans guidance provided in this section is divided into four parts:

- Critical Cyber Asset Classification: The owner operator's categorization of its cyber assets as non-critical or critical is crucial to how the operator is to apply cyber security measures. This identification process is detailed in Section 3.2 Critical Cyber Asset on page 26 below.
- Baseline Cyber Security Measures: The guidance provided in Section 3.3 Baseline Cyber Security Measures on page 27 below is applicable to all cyber assets regardless of their criticality classification. That is, they are to be applied to both critical and non-critical cyber assets.
- Enhanced Cyber Security Measures: The guidance provided in Section 3.4 Enhanced Cyber Security Measures on page 48 below are additional actions on top of the ones defined for non-critical and are applicable to cyber assets identified as critical.
- Existing Planning and Implementation Guidance: There is extensive planning and implementation guidance developed by both industry and government. The Section 3.5 Existing Planning and Implementation Guidance on page 50 below provides a list of reference materials that *should* be used when additional guidance is needed.

3.2 Critical Cyber Asset Classification

Each owner operator *must* develop procedures for identification of control system critical cyber assets. These procedures *must* use consistent criteria to determine asset criticality as described in TSA Pipeline Security Guidelines Section 5.2. To address these procedures this document presents cyber security guidelines in Section 3.3 Baseline Cyber Security Measures on page 27 below that are applicable to all control system cyber assets regardless of their criticality classification. The control system cyber security guidelines in Section3.4 Enhanced Cyber Security Measures on page 48 below present enhanced security measures for control systems cyber assets that have been identified as critical.

Each facility's criticality classification will be used as a baseline to determine the criticality of the cyber assets it contains. Therefore, if a facility is classified as non-critical, by definition, the cyber assets it contains are considered non-critical. Alternatively, if the facility is classified as critical, all cyber assets it contains have the potential, but are not guaranteed, to be critical.

For each critical facility, the operator *must* identify safety, reliability, and/or business continuity objectives. The operators *must* use the following criteria to classify the criticality of cyber assets associated with critical facilities:

- Cyber assets that are necessary to facilities safety and/or reliability objectives are classified as critical cyber assets.
- Cyber assets that are solely associated with business continuity objectives, but not safety or reliability objectives, are not considered critical for the purposes of these guidelines.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 4 and 8.

3.3 Baseline Cyber Security Measures

The following baseline cyber security measures are applicable to all of the operator's cyber assets regardless of their criticality classification.

3.3.1 General Cyber Security Measures

The following are the general cyber security measures that *must* be addressed in the control system cyber security plans section of the CSP:

- Physical access controls to cyber assets
- Monitoring and periodically reviewing remote and third party connections
- Ensure risk assessment of wireless networking before implementation.
- Review, reassessment and update of all procedures annually.
- At a minimum of every 18 months review and reassess cyber asset criticality classification.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 7, 11, and 15.

3.3.1.1 Cyber Asset Physical Access Controls

Physical security *must* be implemented in the INGAA AGA document specifically as it relates to 49 CFR parts 192 and 193, and per the pre-TSA document "Security Practices guidelines Natural Gas Industry Transmission and Distribution", revised May 2008.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 11, 22, and 27.

3.3.1.2 Remote Network Connection Monitoring and Periodic Review

For remote and third party connections used for maintenance and diagnostic purposes the company *must*:

- Establish personnel security requirements including security roles and responsibilities for third-party providers,

- Establish a secure method of monitoring,
- Audit the use, access, and necessity of these connections, and
- Base its monitoring and periodic review on company policy.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 4, 9, 11, 15, 18, 20, 22, 23, and 27.

3.3.1.3 Wireless Network Risk Assessment

Wireless networking technologies are vulnerable to many of the same risks as conventional wired networks; they also have some unique risks that can increase the overall threat surface. As such, wireless networking has an increased level of security concern for control systems. In particular, because wireless networks transmit data through radio frequencies, potential intruders do not need to gain physical access to the network to gain access to the devices and information on the network. A second risk associated with wireless networking is the mobility of the wireless devices. These devices are readily moved beyond the normal safety perimeter and can become exposed to a variety of risks in a less controlled environment.

For this reason, a risk assessment *must* be completed to weigh the benefits of implementing wireless networking against the potential risks for exploitation. Thus:

- Network infrastructure *must* be secured to prevent the unauthorized installation of wireless technology.
- Wireless connectivity *must* be included in network documentation, policies, and procedures.

Further guidance can be found in NIST SP 800-48 and SP 800-97 regarding wireless network security.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 7, 15, 18, and 22.

3.3.1.4 Annual Review, Reassessment, and Update of Control Systems Cyber Security Procedures

There *must* be, at a minimum, an annual review, reassessment, and update of the control systems cyber security plans in accordance with the operator's policy.

Where the responsible entity cannot conform to its own cyber security policy, these instances *must* be documented as exceptions and authorized per company policy.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 8 and 15.

3.3.1.5 Periodic Cyber Asset Criticality Review and Reassessment

The criticality classification of cyber assets as defined in Section3.2 Critical Cyber Asset Classification on page 26 above *must* be reviewed every 18 months, or in accordance with company policy, whichever is less.

The methodology used to define critical assets, the classification of critical assets, and the classification of critical cyber assets *must* be reviewed, approved, and documented according to company policy. Note that this documentation may be subject to review and concurrence as per TSA guidelines.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 4, 6, and 15.

3.3.2 Information Security Coordination and Responsibilities

The information security coordination and responsibilities section of the CSP control system cyber security plan *must* address the following:

- Define a cross-functional cyber security team and an operational framework to ensure coordination, communication, and accountability for information security on and between the control systems and enterprise networks.
- Define information and cyber security roles, responsibilities and lines of communication among the operations, IT, and business groups, as well as with outsourcers, partners, and third-party contractors.
- Establish a system and services acquisition policy, procurement standards, and a process by which potential acquisitions are evaluated against the standards, including encouraging the vendor to follow software development standards for trustworthy software throughout the development lifecycle.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 6 and 9.

3.3.2.1 Control System and Enterprise Network Security Coordination Process.

The company *must* develop and document a network security coordination process. This process *must* include a delineation of roles and responsibilities associated with coordination, communication and accountability of information security on and between the control systems and enterprise networks. The process *must* define information security coordination requirements at every step of the systems development life cycle including strategic planning, design, acquisition, testing, installation, configuration/change management, and retirement.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 9, 13, and 23.

3.3.2.2 Roles, Responsibilities and Lines of Communication Definition

A Cyber Security team *must* establish and document a framework in accordance with company policy that defines the security organization and the roles, responsibilities, and accountabilities of the system owners and users.

Organizational structures vary greatly between companies. Consideration *must* be taken to assure implementation of bi-directional lines of communication no matter what structure is in place. These lines of communication *should* be documented and exercised to test and assure their effectiveness.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, page 4.

3.3.2.3 Procurement Standards

The operator *must* establish a control system and services acquisition policy, procurement standards, and a process by which potential systems, components, and service acquisitions are evaluated against the standards, in accordance with company policy. This includes encouraging the vendor to follow software development standards for trustworthy software throughout the development lifecycle.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 4, 12, and 15.

3.3.2.3.1 System Procurement Standards

The procurement standards *should* address the following security principles when specifying and procuring control system products:

- System Hardening
- Perimeter Protections
- Account Management
- Coding Practices
- Flaw Remediation
- Malware Detection and Protection

See the DHS Cyber Security Procurement for Control Systems, for further guidance. The purpose of DHS's document is to summarize security principles that *should* be considered when designing and procuring control systems products (software, systems, and networks), and provide example language to incorporate into procurement specifications. The security principles in DHS's resource *should* also be applied to any in-house development activities.

3.3.2.3.2 Services Procurement Standards

The procurement standards *should* address the following security principles when specifying and procuring control system services:

- Requires that providers of control system services employ security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements;
- Defines oversight and user roles and responsibilities with regard to external information system services; and
- Monitors security control compliance by external service providers.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 4, 7, and 15.

3.3.3 System Lifecycle

The system lifecycle section of the CSP control system cyber security plans which applies to purchased, operator developed, and/or co-engineered control systems *must* address:

- Incorporation of security measures and controls into the cyber system design and operation for both new system creation and legacy system modification;

- Mitigation strategies for security deficiencies found in control system components;
- Implementation of policies and procedures for the following:
    - Assessment and maintenance of system status and configuration information including tracking changes made to the control systems network, and patching and upgrading operating systems and applications.
    - Secure disposal of equipment and associated media.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 13, 15, and 17.

3.3.3.1 Security Design and Operation of Cyber System

The operator *must* develop and document practices and procedures that incorporate cyber security into the control systems design, modification and operation. Cyber security consideration *should* be part of the initial specification and design of new control systems and all changes to existing systems. In addition, all new control system operation practices and procedures *must* incorporate cyber security consideration and all existing practices and procedures *should* include appropriate cyber security considerations.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, page 15.

3.3.3.1.1 Security Design of Cyber System

The operator *must* consider the following cyber security considerations when designing a new system or making any modifications to an existing system:

- The control system security policy *should* prohibit the embedding of sensitive passwords in source code, scripts, aliases, and short-cuts. If necessary, encryption techniques *should* be used.
- All source code *should* be secured to prevent both its unauthorized viewing and modification. Unauthorized viewing of source code may reveal security deficiencies that may be exploited. Unauthorized modification of source code can result in the introduction of security deficiencies.
- Control systems' hosts and workstations *must* only be used for approved control system activities.
- Any new protocol, application, or software proposed to be added to the control system network *should* be run in a test-bed or development environment to evaluate the potential for impairing the performance of the control system. The evaluation *should* include, but not be limited to, bandwidth requirements, since modern servers and software packages can easily consume WAN capacity at the expense of critical control system traffic.

- The cyber system *must* only grant the minimum set of rights, privileges or accesses required by users, or processes, to perform any control system operation, maintenance, or monitoring task. This applies to all control system components and resources including but not limited to physical access; OS services; files; disks; shared data; networking resources;
- Audit logging *should* be enabled for all devices that are capable. Consideration *should* be given to the secure archiving of all device and system logs.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 11, 13, 15, 18, and 22.

3.3.3.1.2 Security Operation of Cyber System

The operator *should* consider the following cyber security steps in developing control systems operational policies and procedures:

- Periodic review of all rights, privileges and accesses for all users or process to all control system components and resources including but not limited to physical access; OS services; files; disks; shared data; networking resources to insure that unauthorized changes have not been made.
- Review all control systems operational procedures to insure cyber security policies are maintained at design levels. Special emphasis *should* be given to review abnormal operation and emergency operation procedures.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, page 11.

3.3.3.2 Control System Component Security Deficiency Mitigation

Cyber security deficiencies may be identified in control systems hardware and software components. Operators *must* attempt to remediate security deficiencies. In cases where cyber security deficiencies cannot be remediated, mitigation strategies *should* be developed to reduce the risk associated with security deficiencies. The operator *must* develop policies and procedures for addressing hardware and software security deficiencies in control systems.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 15 and 20.

3.3.3.2.1 System Hardening

The operator *must* develop procedures for hardening all components used in control systems. The operator *must* consider the following system-hardening items:

- Secure configurations for all network devices such as firewalls, routers and switches *should* be developed and used to establish baseline configuration for these devices. These configurations *should* be reviewed periodically based on company policy.
- Baseline system configurations including services and ports *should* be periodically reviewed based on company policy to insure that unauthorized changes have not been made.
- Operating system services which are not used by the production SCADA system *should* be removed or disabled to reduce the risk of being exploited.
- The enabled networking protocols on all networked devices should be reviewed and unessential protocols should be disabled. For example IPv6 protocol should be disabled if the network is not IPv6 enabled.
- All required applications and open ports both for normal operation and emergency operation *should* be documented. All ports not in use *should* be disabled.
- Other services *should* be analyzed using a risk assessment to see if the benefits of having them running outweigh the potential for exploitation.
- The remote functions that an operating system provides *should* only be used when necessary and only secure versions *should* be used.
- The use of FTP on a SCADA system *should* be discouraged and strictly controlled. A secure form of FTP *must* be considered.
- Consideration *should* be given to disable or otherwise protect removable media devices (USB ports, CD/DVD drives and other removable media devices).
- All guest accounts *should* be removed.
- All default passwords *should* be modified.
- Unhardened devices *should not* be allowed on the network.
- Secure coding techniques *should* be used when developing applications. The practices *should* include, but not be limited to prevention of buffer overflows, SQL injection, cross-site scripting and other forms of malicious code injection.
- Administrative access to all control systems *must* be strictly controlled.
- Administrative accounts *should* have strong passwords.
- Passwords *should* be changed periodically based on company policy and whenever personnel changes dictate.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 13, 15, 17, and 18.

3.3.3.2.2 Software Patches and Updates

The operator *must* develop policies and procedures for management of software patches and updates, anti-virus software and anti-malware software. All policies and procedures *should* be developed in accordance with the control system supplier's recommendations.

- The operator *should* apply all critical control system supplier approved operating system updates in accordance with company policy.

- Anti-virus, anti-malware and other protection software *should* be used in accordance with the control system supplier's recommendations.
- Anti-virus, anti-malware and other protection software *should* be updated in accordance with the control system supplier's recommendations.
- The operator *should* periodically inventory the software patch level of all systems on the network to be aware of un-patched systems base on company policy.
- The operator *should* ensure that critical application and database security patches are applied in accordance with the control system supplier recommendations.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 13, 15, and 22.

3.3.3.3 Change Control Policies and Procedures

Change control is a system of processes, with appropriate controls and documentation intended to evaluate change activities for their potential impacts prior to implementation. It *should* address any change that will impact the pipeline control system whether permanent or temporary. Change control incorporates planning for these situations and considers their unique requirements.

Document control *must* be properly administered. Maintaining a record of changes to the control system will provide a better understanding of the system and identify possible threats to its integrity. The records *must* be complete, accurate, and accessible only to authorized personnel. Records *must* be retained in accordance with the company's policies.

The operator *should* consider a baseline change approach that fully documents the control system configuration. The baseline configuration *should* document all information pertaining to the control system to a level of specificity that would allow it to be restored. Any planned change to the baseline configuration *should* include procedures to recover the baseline in the event of unexpected impacts or failures. Each approved change to the baseline *must* be documented.

Process Steps

The process steps that *should* be followed and documented when managing control system changes follow:

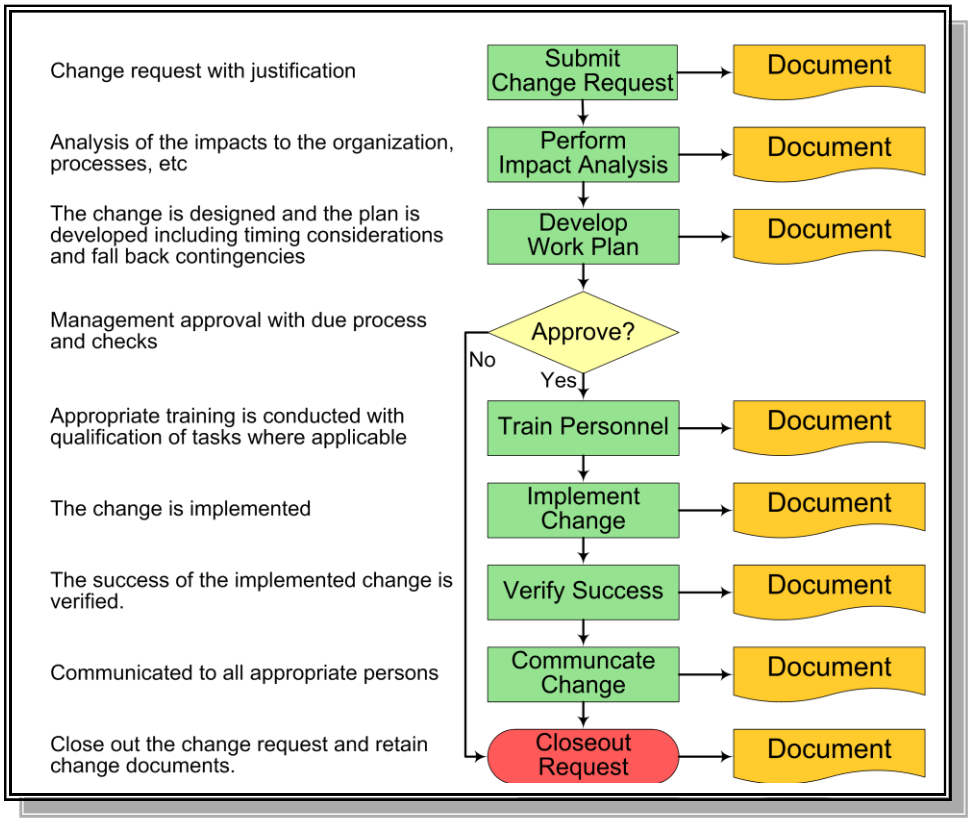

Change request with justification
Submit Change Request
Document
Analysis of the impacts to the organization, processes, etc
Perform Impact Analysis
Document
The change is designed and the plan is developed including timing considerations and fall back contingencies
Develop Work Plan
Document
Management approval with due process and checks
Approve?
No
Yes
Appropriate training is conducted with qualification of tasks where applicable
Train Personnel
Document
The change is implemented
Implement Change
Document
The success of the implemented change is verified.
Verify Success
Document
Communicated to all appropriate persons
Communcate Change
Document
Close out the change request and retain change documents.
Closeout Request
Document

Figure 8: Cyber Security Change Control Process Flow Chart

- **Request**: A method for formally requesting control system changes *must* exist. It *should* document the origination and reason for the change.
- **Analysis**: Each change *must be* analyzed for control system impact and risk prior to implementation. This process step *should* include a review of the proposed change to ensure the integrity and security of the control system is not degraded by the change.
- **Work Plan Development**: A work plan *must* be developed by the appropriate personnel and use appropriate policies and procedures. A properly developed work plan *must* include how the change will be scheduled, implemented, verified, and communicated.
- **Approval**: An approval process *must* be in place which *should* include a review of the impact analysis.
- **Training**: Training *should* be provided for all affected parties to ensure personnel understand and adhere to the changed condition.
- **Implementation**: The change *must* be implemented in accordance with the pre-approved work plan. Any deviation from the original work plan *should* be re-submitted to the change control process. All planned control system changes *should* be implemented and evaluated in a non-production environment prior to implementation in the production environment.
- **Verification**: The change *must* be verified that the actual outcome is in alignment with expected results.
- **Communication**: All changes *must* be communicated to all affected parties.

- **Closeout**: Any changes implemented in the control system baseline *must* be documented. All change control documentation *must* be retained in accordance with company policy.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 15 and 22.

3.3.3.4 Secure Equipment and Media Disposal Policies and Procedures

The operator *must* establish policies and procedures for the secure disposal of equipment and associated media.

The policies and procedure *must* include the sanitization of information system media, both digital and non-digital, prior to disposal or release for reuse. Sanitization is the process used to remove information from cyber system media such that there is reasonable assurance, in proportion to the confidentiality of the information, that the information cannot be retrieved or reconstructed.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 13, 15, and 18.

3.3.4 System Restoration and Recovery

The system restoration and recovery section of the CSP control system cyber security plans *must* address plans and preparation for the return to full service of unavailable, degraded, or compromised control systems in a timely fashion as defined by the organization consistent with their availability and recovery requirements.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 15, 26, and 33.

3.3.4.1 Control Systems Restoration and Recovery Plan

Operators *must* plan and prepare for the prompt restoration and recovery of a failed or compromised SCADA system. Recovery may involve other affected interfaces or interdependent systems such as power, communications, and human operators.

Restoration and recovery plans are designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster. These plans *should* dictate contingencies, business resumption, disaster recovery and/or technical recovery specifics based on the organization needs in operation for safety, reliability and/or financial concerns.

The plans *must* include the following:

- Contingencies for cyber threats, natural disasters and/or equipment/software failures.
- Procedures for restoring systems from backups.
- Employee training to insure familiarization with the contents of the plans.
- Define the roles and responsibilities of responders.

- Communication procedures and list of personnel to contact in the case of an emergency including control system vendors, network administrators, control system support personnel, etc.

Additionally, the plans *should* include the following:

- Procedures for validating system backups.
- References to current configuration information on all systems requiring restoration.
- Specifications of recovery time objectives and specific contingency plan objectives if recovery times are exceeded.
- Required response to events or conditions of varying duration and severity that would activate the recovery plan.
- Personnel list for authorized physical and cyber access to the control system.
- Requirements for the timely replacement of components in the case of an emergency. If possible, replacements for hard-to-obtain critical components *should* be kept in inventory.

This plan *should* also be reviewed periodically according to company policy.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 15, 17, 31, 33, 34, and 35.

3.3.4.2 Control Systems Restoration and Recovery Process

Operators *must* make and secure backups of critical system software, including applications, data, and configuration information, on a regular basis as defined by company policy consistent with their availability and recovery requirements.

Installation media and license information *should* be kept in a secure location.

The restoration and recovery process *must* be:

- Tested periodically according to company policy.
- Executed on a frequency according to company policy.
- Reviewed and refined as necessary according to company policy.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 31, 34, and 35.

3.3.5 Intrusion Detection & Response

The intrusion detection and response section of the CSP control system cyber security plans *must* address the implementation of policies and procedures for cyber intrusion monitoring, detection, incident handling, and reporting.

The operator *must* establish policies and procedures for cyber intrusion monitoring and detection as well as incident handling and reporting.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 15 and 20.

3.3.5.1 Cyber Intrusion Monitoring and Detection Policies and Procedures

Operators are responsible for monitoring and logging system activity for the purpose of discovering security events. To detect cyber intrusions into its control systems, operators *must* establish policies and procedures for monitoring its control systems.

Beyond the implementation of cyber protection technology, the following system information *must* be reviewed on a periodic basis, as defined in the operator's control system cyber security plan.

These monitoring procedures *should* include, but are not limited to, the following:

- Unexpected log file events;
- Unusually heavy network traffic;
- Out of disk space or significantly reduced free disk space;
- Unusually high CPU usage;
- Creation of new user accounts;
- Attempted or actual use of administrator-level accounts;
- Locked-out accounts;
- Account in-use when the user is not at work;
- Cleared log files;
- Full log files with unusually large number of events;
- Antivirus alerts;
- Disabled antivirus software and other security controls;
- Unexpected patch changes;
- Machines connecting to outside IP addresses;
- Requests for information about the system (social engineering attempts);
- Unexpected changes in configuration settings, and
- Unexpected system shutdown.

Additionally the operator *should* evaluate the use of an Intrusion Detection System (IDS) to monitor the behavior of the network in order to identify events that may be considered unusual or undesirable. A properly configured IDS can greatly enhance the security management team's ability to detect attacks entering or leaving the system, thereby improving security. They can also potentially improve a control network's efficiency by detecting non-essential traffic on the network.

Passive IDS *should* be implemented and thoroughly reviewed well in advance of enabling an active Intrusion Prevention System (IPS).

In view of the unique protocols that may be implemented in a SCADA system, any use of IPSs *must* be carefully examined to ensure that safe and reliable system operation is not compromised by automated actions of the IPS.

Personnel *must* have management authorization before they perform control system security evaluations and/or use network testing & monitoring software.

All operator employees *must* watch for and report immediately any potential security incident including a virus, an intrusion, and an out-of-compliance situation using the operator's incident handling and reporting policies and procedures.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 18, 22, and 23.

3.3.5.2 Cyber Intrusion Incident Handling Policies and Procedures

Operators *must* be prepared to respond quickly and effectively when control system security defenses are breached. The operator's incident response policy is the foundation of the incident response program. It defines which events are considered incidents, establishes the organizational structure for incident response, and defines roles and responsibilities.

The incident response plan provides a roadmap for implementing an incident response program based on the company's policy. The plan *should* indicate both short- and long-term goals for the program, including metrics for measuring the program. The incident response plan *should* also indicate how often incident handlers should be trained and the requirements for incident handlers. The incident response plan is the formal documentation of a predetermined set of roles and responsibilities and instructions or procedures used by the personnel assigned those roles to be prepared for, detect, respond to, limit consequences from, recover from, and follow up to incidents against the organization's cyber and/or specific control systems.

The selection criteria of the members of the incidence response team should ensure they have the appropriate skills. The credibility and proficiency of the team depend to a large extent on the technical skills of its members. Poor technical judgment can undermine the team's credibility and cause incidents to worsen. Critical technical skills include system administration, network administration, programming, technical support, and intrusion detection. Teamwork and communications skills are essential for effective incident handling.

The incidence response team *should* identify other groups with the organization that may need to participate in incident handling. Every incident response team relies on the expertise, judgment, and abilities of other teams, including, but not limited to, management, information security, IT, legal, public affairs, and facilities management.

The reaction to an incident *should* be a measured response. The response *should* be dependent upon the level of criticality of the compromised components, not simply the system that was compromised. If an incident is discovered, there *should* be an initial risk assessment performed to evaluate the effect and impact of both the attack as well as the options to respond. That is, the responders *should* be cautioned not to over- react as that has the potential of compromising the integrity, reliability, and safety of the control system more than the incident itself.

The incident response procedures provide detailed steps for responding to an incident. The procedures should cover all the phases of the incident response process. The procedures *must* be based on the operator's incident response policy and plan.

Incident Response Plans *should* include the following:

1) Roles and Responsibilities Definition:

All system stakeholders have responsibilities related to its security of the computing systems and networks. Each stakeholder has specific responsibilities with regard to the reporting and handling of cyber security incidents. It is critical for each entity to know in advance its role. This includes all stakeholders of the information the system generates, transmits, receives, contains, and maintains. These roles *should* include:

a) Security Personnel;

b) Management;

c) Information Security Liaison;

d) System Administrators, and

e) System Users

Each of these roles has a responsibility in monitoring, detecting, and responding to cyber security incidents and *should* be included in the plan.

2) Declaration of Preparation:

Being prepared to respond to an incident before it occurs is one of the most critical facets of incident handling. This advanced preparation avoids disorganized and confused responses to incidents. It also limits the potential for damage by ensuring that response plans are familiar to all staff, thus making coordination easier. The items that have been put in place to prepare for an incident *should* be highlighted in this section. These *should* include:

a) Baseline Protections: Highlight the items that have been deployed throughout the corporation that act as the first line of defense.

b) Planning and Guidance: This section *may* include descriptions of the incidence response security team availability, how and when they can be contacted and backup methods of initial notification and/or continuing communications if an incident adversely affected regular communications.

c) Incident Response Training: Incident response training for personnel and testing incident response capability for an information system is crucial to the successful execution of any incident response plan and *should* be include in the plan itself including training frequency and success criteria.

3) Incident Response Phases Definition: This section defines how the organization methodically addresses cyber security incidents. It *should* include:

a) **Alert Phase:** The alert phase is the process of learning about a perceived or real cyber security incident, and reporting it to the company's cyber security response team.

b) **Triage Phase**: The triage phase is the process of examining the information available about the incident to determine first if it is a "real" incident, second, if it is real, its severity, and third, committing the proper resources to respond to the incident.

i) **Identification**: This involves validating the incident, identifying its nature, and classifying the type of incident. Although cyber security incidents may take many forms and involve many devious means, certain types of attacks occur more frequently than others. Knowing what these types of attacks are and how the organization counters them will help its staff to be prepared to react and report all related information to the appropriate parties and organizations.

ii) **Incident Severity**: A formalized definition of the severity levels which *may* include number or servers, system, or services that are affected. The severity will dictate how many and which types of resources are employed.

iii) **Incident Declaration**: Incident declaration is a procedure by which an authorized security member documents that an incident has or is occurring and the appropriate resources, based on its severity are pressed into action.

c) **Response Phase:** In the response phase, evidence is gathered and analyzed to determine the cause of the incident, the vulnerability or vulnerabilities being exploited, how to contain the scope and magnitude of an incident, and eliminate these vulnerabilities and/or stop the incident.

i) **Incident Evidence Handling:** The collection, maintenance, and tracking of the evidence is a critical step. This also includes protecting the evidence.

ii) Containment: The immediate objective for the containment stage is to limit the scope and magnitude of an incident as quickly as possible, rather than to allow the incident to continue in order to gain evidence for identifying and/or prosecuting the perpetrator.

iii) **Eradication**: The next priority, after containing the damage from a cyber security incident, is to remove the cause of the incident.

d) **Recovery Phase:** This is the restoration of a system to its normal mission status. This phase usually starts once the response phase is complete but in some situations *may* overlap.

e) **Maintenance Phase:** Following up on an incident after Recovery helps to improve incident handling procedures. This stage *may* include:

i) Response quality review and documentation;

ii) Incident Costs review and documentation;

iii) Incident Report Filing, and

iv) Revision of Policies and Procedures.

Appendix B – Cyber-Security Incident Response Plan Example on page B-1 below is a model that may be used as a template to create an organization's Cyber Security Incident Response Plan. It contains the items that *should* be included but each operator must evaluate and prepare their Cyber Security Incidence Response Plans based on their own unique needs, circumstances, and resource commitments. The security incident responses in this example are only provided to spur thought and conversation among an organization's subject matter experts and policy makers.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 15, 18, 23, 26, 27, 29, 30, 31, 33, 34, and 35.

3.3.5.3 Cyber Intrusion Incident Reporting Policies and Procedures

Operators *must* be prepared to respond quickly and effectively when control system security defenses are breached. The incident response policy is the foundation of the incident response program. It, among other items, lists the requirements for reporting incidents.

The company may be required to communicate incident details with outside parties, such as the media, law enforcement agencies, and incident reporting organizations. The incident response team should discuss this requirement at length with the company's public affairs office, legal department, and management to establish policies and procedures regarding information sharing. The team *must* comply with the company's existing policy on interacting with the media and other outside parties.

All potential security incidents *must* be reported using the operator's incident reporting policies and procedures.

Log files and any other information containing system security relevant events are important for error correction, security breach recovery, investigations, and related efforts. These logs *must* be

- Retained for a period as defined by the company's retention policy;
- Secured to prevent modification, and
- Secured so only authorized personnel are able to review these logs.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 22, 27, 34, and 35.

3.3.6 Training

The training section of the CSP control system cyber security plans *must* address implementation of

- Information security awareness training for all users of control systems;
    - ➢ Before permitting access to the control systems and,
    - ➢ Annually or sooner as necessitated by changes in the control system.
- Targeted control systems security-related training for individuals with control system security responsibilities;

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, page 12.

3.3.6.1 Information Security Awareness Training

An information security awareness training program for all control systems users must be implemented.

Information security awareness training *must* be performed as follows:

- Prior to accessing control systems;

- On an annual basis, and
- As necessitated by changes in the control system.

Training should include, but is not limited to, the topics listed below:

- Corporate security policy and compliance;
- Incident Response Plan;
- Protect information subject to confidentiality concerns;
- Password rules and management;
- Malicious code protection;
- Email use and protection policies;
- Corporate web usage;
- Information mining techniques including social engineering and shoulder surfing;
- Change control policies and procedures;
- Configuration management policies and procedures;
- Inventory and property transfer policies and procedures;
- Laptop and other mobile device security;
- Software license requirements;
- Authorized software on control systems;
- Access control issues;
- Individual accountability;
- Visitor control and physical access to spaces, and
- Desktop security.

Detailed information regarding awareness and training can be found in NIST–SP800-50 "Building an Information Technology Security Awareness and Training Program"

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, page 12.

3.3.6.2 Control Systems Security-Specific Training

Individuals with significant control systems security-related roles must have control systems training specific to their roles. This training should include the following:

- Access controls;
- Password controls;
- Group Policy Objects;
- Firewall rules;
- Segregation of duties;
- Incident handling;
- System restoration and recovery;
- Vulnerability and assessment;
- Critical site identification;
- Intrusion detection and response, and

- Physical access.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, page 12.

3.3.7 Functional Segregation and Access Control

The functional segregation and access control section of the CSP control system cyber security plans *must* address:

- Segregation and protection of the control systems network from the business network and the Internet through the use of firewalls and other protections. This applies to both wired and wireless networks.
- The operator *should* consider physical segregation and/or separation of control system servers to dedicated racks or data center floor space.
- Using control systems hosts and workstations only for approved control system activities.
- Enforcement of access controls for local and remote users, guests, and customers.
- Implementation of procedures and controls for approval and policy enforcement for remote and third-party connections to control networks.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, page 11.

3.3.7.1 Control System Functional Segregation

Control system functional segregation consists of separating the control system from the business network and isolating it from the internet. It also includes segregating the control system's network from other networks within the data center. In addition, the control system *must* be segregated in functionally so that its only use is for approved control system activities.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 11, 13, and 15.

3.3.7.1.1 Baseline Control System Segregation

The operator *must* segregate the control system from the business network and the internet through the use of various protection mechanisms such as firewalls, VLANs, or access lists.

Implementation of these segregation techniques may reduce control system network reliability. Consideration *must* be taken to ensure the data and network used by production control systems remain reliable. The following considerations *should* be taken into account:

- A minimum bandwidth requirement for control systems;
- Redundancy;
- Diversity of communication paths, and
- Latency.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, page 11.

3.3.7.1.2 Data Center Network Segregation

The operator *must* segregate the SCADA network from other networks within the data center.

There *must* be minimal access points between the production SCADA network and the corporate network. All access points *must* be documented.

Firewalls *must* be configured based on the operator's policies to provide adequate protection from outside network access and adequate protection for the control network. The firewalls *should* be configured with the following features:

- Only allow explicitly authorized incoming traffic;
- Only allow explicitly authorized outgoing traffic;
- Activate anti-spoofing devices;
- Activate connection time-outs;
- Deny ICMP requests, and
- Activate logging and reporting of unauthorized traffic.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 11 and 22.

3.3.7.1.3 Control System Usage Approval

Operator *must* develop policies and procedures to ensure the control systems' hosts and workstations are only used for approved control system activities.

These *should* include the following:

- A documented baseline configuration of all required control systems' operating system services.
- All operating system services not required for approved control system operation *must* be disabled.
- A documented baseline configuration of all authorized executable control systems' application software.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 15, 18, and 22.

3.3.7.2 Baseline Access Controls

The following access controls apply to all cyber assets regardless of their criticality classification.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 11 and 22.

3.3.7.2.1 Physical Access Control to Control Systems and Control Networks

The operator *must* implement physical access controls as specified for non-critical facilities in the INGAA Pipeline Security Practices Guidelines Natural Gas Pipeline Industry Transmission and Distribution.

Field components such as HMI, PLC, RTU, *must* be installed using physical security measures, such as a locked cabinet or building, to mitigate any absence of logical security controls.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 11 and 15.

3.3.7.2.2 Logical Access Control to Control Systems and Control Networks

The operator *must* implement the following logical access controls as specified for non-critical facilities:

- Only authorized workstations *must* be connected to the network;
- User access approval *must* be requested as per operator's policies and procedures;
- Management or proxy *must* approve changes in the level of access;
- Third party connections *must* be explicitly authorized;
- Third party connections *must* be disabled when not in use;
- Devices *must* be secured with a password when capable, and
- Devices *must not* use the default password provided by the vendor.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 11 and 18.

3.3.7.2.3 Access Control Enforcement

The operator *must* develop policies and procedures to monitor and enforce compliance with all operator-developed control network access controls.

Access controls enforcement procedures *must* include periodic review and audit in accordance with operator's policies. The audit and review *should* ensure compliance that the following have explicit authorization:

- Enabled operating system services;
- Remote connections to control systems networks;
- Granted access and privileges;
- Active Firewall rules and configuration;
- Devices connected to the network;

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 11, 15, and 18.

3.4 Enhanced Cyber Security Measures

The following enhanced cyber security measures are applicable only to the operator's cyber assets that have been classified as critical.

3.4.1 Access Control

The enhanced access control section of the CSP Control system cyber security plans *must*:

- Restrict physical and logical access to control systems and control networks through the use of an appropriate combination of locked facilities, passwords, communications gateways, access control lists, authenticators, and separation of duties, invocation of least privilege, and/or other mechanisms and practices.
- Implement a risk assessment to weigh the benefits of implementing wireless networking against the potential risks for exploitation. Enhanced networking control technologies *should* be considered for wireless before implementation.

The following access controls apply to cyber assets that have been classified as critical as defined in Section3.2 Critical Cyber Asset Classification on page 26 above.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 11 and 15.

3.4.1.1 Physical Access Control to Control Systems and Control Networks

The operator *must* implement physical access controls as specified for critical facilities in the INGAA Pipeline Security Practices Guidelines Natural Gas Pipeline Industry Transmission and Distribution.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 11, 22, and 23.

3.4.1.2 Logical Access Control to Control Systems and Control Networks

The operator *must* implement logical access controls. Guidance is provided below:

- Initial access to the system *must* first be granted to a secure corporate network, and then granted to the control system from that point.
- Network ports not in use *should* be disabled to minimize unauthorized access.
- Multiple access levels *should* be defined which may include viewer, gas controller, developer and system administrator roles.
- Changing the ID or account from the default for these devices *should* also be considered.
- Two-factor authentication *should* be considered for access into the control system and/or networks.

3.4.1.3 Wireless Network Risk Assessments

Operators *must* develop a risk assessment process before deploying wireless network devices. The risk assessment process *must* address the unique risks associated with wireless network devices and detail the steps to be taken to mitigate these risks to an acceptable level. These policies and procedures *must* detail the benefits and risks associated with a wireless networking technology implementation.

Operators *must* also develop policies and procedures for the design, development, implementation and ongoing security review of wireless technologies. These policies and procedures *should* include the following considerations:

- Review and change factory default settings as appropriate on all devices.
- Inventory and control all access points and maintain a full understanding of the topology of the wireless network.
- Implement the most secure capabilities available on all devices.
- Install firewalls between wired and wireless devices.
- Block all unapproved services and ports.
- Use strong cryptography.
- Minimize data broadcast distances.
- Label and keep inventories of the fielded wireless and handheld devices.
- Create backups of data frequently.
- Perform periodic security testing and assessment of the wireless network.
- Perform ongoing, randomly timed security audits to monitor and track wireless and handheld devices.
- Apply software and firmware patches and security enhancements.
- Monitor the wireless industry for changes to standards that enhance security features and for the release of new products.
- Monitor wireless technology for new threats and vulnerabilities.

Further guidance can be found in NIST SP 800-48 and SP 800-97 regarding wireless network security.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 4, 7, 18, and 22.

3.4.2 Security Vulnerability Assessment

The security vulnerability assessments section of the CSP control system cyber security plans *must* include the process to execute control system SVAs periodically on a non-production environment with the following criteria:

- The SVA *should* include testing as appropriate in a non-production environment;
- The time between control system SVAs *must not* exceed 36 months;

Security vulnerability assessments provide insight into the potential and actual risks of penetration and exploitation of SCADA and Control Systems networks. These assessments provide information required to mitigate the risk exploitations prior to their occurrence.

Prior to performing the assessment subject matter experts and stakeholders *should* be identified and the scope of the assessment defined.

A Security Vulnerability Assessment process *should* include procedures similar to the ones listed below:

- Identify Potential SCADA cyber security threat sources using a combination of industry standards (such as NIST 800-82) and company subject matter experts;
- Identify Vulnerabilities the potential threats may exploit; failure modes and causes, to define a set of risks;
- Determine each raw risk's likelihood;
- Determine each raw risk's magnitude of Impact;
- Identify all existing controls that mitigate the risks to any degree;
- Determine maturity level of existing controls;
- Calculate overall/residual risks;
- Obtain consensus from all participants;
- Evaluate enhanced control options;
- Perform cost benefit analysis for control enhancements;
- Select most cost beneficial controls based on risk acceptance level;
- Implement selected controls;
- Implement control effectiveness monitoring program (self assessment, all non-passive testing *should* be conducted in a non-production environment);
- Take actions based on self assessment results of control effectiveness, and
- Re-evaluate the risk assessment within the time period required.

*For additional guidance issued by NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, please refer to Appendix F, pages 7, 15, 22, 23, and 30.

3.5 Existing Planning and Implementation Guidance

The following is a list of planning and implementation guidance developed by both industry and government:

- AGA Report Number 12, *Cryptographic Protection of SCADA Communications,* Part 1: Background, Policies and Test Plan
- American Petroleum Institute, API 1164 *Pipeline SCADA Security*
- Chemical Industry Data Exchange (CIDX), *Guidance for Addressing Cybersecurity in the Chemical Sector*
- Department of Homeland Security, *Catalog of Control Systems Security: Recommendations for Standards Developers*, January 2008
- ISA-99 Manufacturing and Control Systems Security
- ISA-99-1 Concepts, Models and Terminology

- ISA-99-2 Establishing a Manufacturing and Control System Security Program
- National Institute of Standards and Technology (NIST) SP800-82, *DRAFT Guide to Industrial Control Systems (ICS) Security*
- National Institute of Standards and Technology (NIST) SP800-48, *Wireless Network Security, 802.11, Bluetooth, and Handheld Devices*

Appendix A – Recurring Actions

RECURRING ACTIONS				
	12 Months	18 Months	36 Months	Other
Baseline Cyber Security Measures	Perform an annual review of the control system cyber security plan and update as required. (Control System Cyber Security Procedures 3.3.1.4)	Conduct / update cyber asset criticality assessments on a periodic basis, not to exceed 18 months. (Cyber Asset Criticality 3.3.1.5)		Periodically review remote and third party connections (Remote Network Connections 3.3.1.2)
	Conduct annual information security and control system training for appropriate personnel. (Training 3.3.6.1)			Periodic review of all rights, privileges and accesses for all users or processes (Security Operation 3.3.3.1.2, Access Control Enforcement 3.3.7.2.3)
				Periodic review of security configurations of all network devices (System Hardening 3.3.3.2.1)
				Periodic review of baseline system configurations (System Hardening 3.3.3.2.1)
				Periodically change passwords based on company policy or whenever personnel changes dictate (System Hardening 3.3.3.2.1)
				Periodically inventory the software patch level of all systems (Software Patches and Updates 3.3.3.2.2)
				Periodically review and test restoration and recovery plans and processes (Control Systems Restoration and Recovery 3.3.4.1 and 3.3.4.2)
				Periodic review of systems information (Intrusion Monitoring and Detection 3.3.5.1)

RECURRING ACTIONS				
	12 Months	18 Months	36 Months	Other
Enhanced Cyber Security Measures			Conduct periodic control system vulnerability assessments SVAs, not to exceed 36 months. (Security Vulnerability Assessment 3.4.2)	Backup wireless configuration data frequently (Wireless Network Risk Assessment 3.4.1.3)
				Periodic security testing and assessment of the wireless network (Wireless Network Risk Assessment 3.4.1.3)
				Ongoing randomly timed security audits of wireless and handheld devices (Wireless Network Risk Assessment 3.4.1.3)
				Ongoing monitoring of wireless technology and industry standards for vulnerabilities and enhanced security features (Wireless Network Risk Assessment 3.4.1.3)
Note: Baseline measures apply to all cyber assets. Enhanced measures apply in addition to baseline measures for cyber assets classified as critical.				

Appendix B – Cyber-Security Incident Response Plan Example

Special Note:

The following is an example and should only be used as such. Each operator must evaluate and prepare their Security Incidence Response Plans based on their own unique needs, circumstances, and resource commitments. The security incident responses in this example are only to spur thought and conversation among an organization's subject matter experts and policy makers and are not intended to be used in part or in whole without careful consideration.

Control Systems Cyber Security Working Group

Cyber-Security Incidence Response Plan Example

Release Date: January 31, 2011
Version: 1.0

10 G Street, Suite 700
Washington DC 20002
Phone: (202) 216-5900
Fax: (202) 216-0876
Website: http://www.INGAA.org/

Proprietary Notice

ADDITIONAL NOTICE

The following information describes your rights and obligations regarding this publication.

This publication contains information pertinent to specific product(s) and/or program(s). You are authorized to use this information for the express purpose of using the product(s) and/or program(s) described herein. The following rules apply to this authorization.

All brand and product names referred to in this document are trademarks or registered trademarks of their respective companies. INGAA has obtained permission to use/reproduce information from companies whose products or information are referenced or duplicated here. If you have not purchased the actual products to which this document refers, then the information referred to here is not available/applicable to you and you should refer to your specific product information.

This publication may include technical inaccuracies or typographical errors. If you are aware of inaccuracies or errors, notify INGAA. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. INGAA may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time.

Issue Date: January 1, 2011

Revision Date: January 1, 2011

Printed in the United States of America

INGAA Proprietary Information

This document contains information that is confidential and proprietary to INGAA its affiliates, subsidiaries, suppliers, and/or third parties, and may not be disclosed except under obligations of confidentiality and subject to the provisions of a Non-Disclosure Agreement between the proposed recipient and INGAA or any of its affiliates, as applicable, or without the prior written consent of INGAA.

Revision History

Author	Change No.	Revision Date	Revision Summary
CSCSWG	0	Dec. 10, 2010	Draft Release

Table of Contents

Section **Page**

INGAA Proprietary, Confidential, and Sensitive Security Information (SSI)

This page intentionally left blank.

1 INTRODUCTION

1.1 How to Use This Document

The following is an example and should only be used as such. Each operator must evaluate and prepare their Security Incidence Response Plans based on their own unique needs, circumstances, and resource commitments. The security incident responses in this example are only to spur thought and conversation among an organization's subject matter experts and policy makers and are not intended to be used in part or in whole without careful consideration.

1.2 Purpose

The purpose of this security incident response plan is to provide general guidance to (*Company name*) staff - both technical and managerial - to: enable quick and efficient recovery from security incidents; respond in a systematic manner to incidents and carry out all necessary steps to correctly handle an incident; prevent or minimize disruption of critical computing services; and minimize loss or theft of sensitive or mission critical information.

It is also a guide to sharing information with other organizations — internally within (*Company name*), and externally with other information security and law enforcement organizations.

1.3 Scope

The guidance contained in this document is applicable to all (*Company name*) employees and consultants, collectively known as (*Company name*) users, and others who process, store, transmit, or have access to IT information and infrastructure computing resources. This guidance is applicable to all company information and infrastructure computing resources at all levels of sensitivity.

2 ROLES AND RESPONSIBILITIES

Each staff member has responsibilities related to the security of all company's computing systems and networks, including control systems. The persons and units listed below have specific responsibilities with regard to the reporting and handling of information security incidents. It is important for each entity to know in advance its role.

2.1 *Security Team Name*

(*Security Team Name*) is the unit within (*Company name*) that is responsible for managing information security standards, procedures, and controls intended to minimize the risk of loss, damage, or misuse of supported electronic data.

(*Security Team Name*):

- Serves as the focal point for reviewing information system security issues that have company-wide impact;
- Establishes and maintains the security incident response plan;
- Handles and investigates all information security problems/incidents;
- Works with information security liaisons and/or other system administrators to analyze and resolve security incidents;
- Evaluates and documents investigation findings after resolving an incident;
- Recommends security technology and tools (e.g. use of intrusion detection tools, penetration testing, etc) to appropriate executive management , and
- Promotes security awareness to the company's computing community.

2.2 Management Advisory Board

The management advisory board is made up of senior managers from the company's (*IT organization*) and other internal business functions. The organization representatives are (*Network Services, Information Risk Management, Control System Operations, Server Operations, Desktop Operations, and Help Desk)*. Other internal business functions represented include (*Corporate Security, Legal, Human Resources, Media Relations, and Disaster Recovery)*. This group makes decisions and budget requests above the level delegated to the (*Security Team Name*) Security Manager.

2.3 Security Manager

The Security Manager is responsible for:

- Coordinating the overall response and recovery activities for security incidents;
- Providing guidance and assistance in determining the appropriate action taken;
- Updating management of incident investigation findings;
- Notifying upper management of significant incidents;

2.4 Information Security Liaison

Departments that may be impacted by a cyber security incident will designate an Information Security Liaison who will participate in the analysis and resolution of security incidents that impact their area of responsibility.

2.5 System Administrators

System Administrators may often be the first to discover a security incident. System administrators are responsible for reporting incidents to (*Security Team Name*) immediately, as well as helping to determine and implement a solution, when applicable.

System Administrators should perform the following if there is a suspicion that a security incident has occurred, is occurring, or is planned:

- Investigate briefly;
- If suspicion is confirmed or indeterminate, confer with supervisor, networking manager/administrator, and notify (*Security Team Name*) immediately;
- Start an event log by noting date and time of all actions;
- Take snapshot of pertinent files within the first half hour of incident investigation;
- Identify risk to system or information;
- Implement incident discovery step of response plan upon request or when appropriate;
- Monitor, study and update situation.

2.6 Users

Despite advances in automated intrusion detection systems, computer users may be the first to discover an intrusion. Both end and system users should:

- Be vigilant for unusual system behavior, which may indicate a security incident in progress;
- Report suspected or known incidents such as a virus infection, a system compromise, or a denial of service incident, which may be detected by resident software on the system user's workstation to (*Security Team Name*);
- Preserve evidence;
- Cooperate with investigative personnel during investigation if needed.

3 Preparation

(*Company name*) considers being prepared to respond to an incident before it occurs as one of the most critical facets of incident handling. This advanced preparation avoids disorganized and confused responses to incidents. This minimizes the risk of causing more harm than good by making poor uniformed, uncoordinated actions in response to the incident. It also limits the potential for damage caused by the incident itself by ensuring that response plans are familiar to all staff, thus making coordination easier.

3.1 Baseline Protection

The company has installed baseline protection on all systems and networks. All computing components have a first-line level of defense to keep incidents from spreading quickly from system to system.

All system administrators must maintain compliance with United States Computer Emergency Readiness Team (US-CERT) notices, bulletins, and incident and vulnerability notes to ensure that all appropriate defensives are in place before an incident occurs.

The company has obtained tools in advance to avoid the potentially damaging delays that can occur when starting to procure such tools after an incident has happened. Examples include virus detection and eradication tools.

3.2 Planning and Guidance

The company has established a Security Team: (*Security Team Name*). Assigned security personnel will be available during a critical incident involving one or more essential systems.

The company has planned for emergency communications needs. Should an incident adversely affect regular communication channels, a list has been created of personnel to be contacted during incidents, including home phone numbers, cell phones and pager numbers.

The company has created this written incident response plan and distributed it to all appropriate staff. This written guidance is structured to help the staff respond to unexpected events that may be symptoms of computer security incidents.

3.3 Training

Appropriate training is provided to all security personnel and other appropriate staffs on a regular basis. Training helps update their knowledge and skills in handling security incidents.

4 PROCEDURES FOR RESPONDING TO INCIDENTS

(*Company name*) defines five phases of response when servicing a computer security incident: Alert; Triage; Response; Recovery; and Maintenance. Knowing about each stage facilitates responding more methodically and efficiently, and helps key staff understand the process of responding.

4.1 Alert Phase

The alert phase is the process of learning about a perceived or real security incident, and reporting it to the (*Security Team Name*). Alerts may arrive from a variety of sources including: firewalls and intrusion detection systems, anti-virus software, threats received via electronic mail, media reports about a new threat, etc. The (*Security Team Name*) is notified by the "hotline" telephone number, or the duty phone/pager that is reachable 24 hours a day, 7 days a week.

If a computer-based incident is detected, it must be reported immediately to (*Security Team name*). In particular, each system user or system administrator must know how and when to contact the security team.

In addition, (*Security Team name*) has the responsibility to report incident information to senior management in a timely fashion. The system and network audit logs provide sufficient information to facilitate deciding whether or not unauthorized activity has occurred. In the event of a serious breach of security or evidence of criminal activity, the (*Security Team Name*) Security manager will notify senior management.

WARNING: No staff member, except the designated company spokesperson, has the authority to discuss any security incident with any person outside the company.

4.2 Triage Phase

The triage phase is the process of examining the information available about the incident to determine first if it is a "real" incident, and second, if it is, its severity. The Security Manager does this, with assistance from the permanent team members. If the incident's severity warrants, the management advisory board will also be alerted. The board will do two important things in this phase:

- A decision to "pursue" or "protect" will be made. That is, does the company want to attempt to catch the perpetrator(s) of the attack for later criminal or civil action, or does it simply want to stop the incident and restore normal operations? This decision must be made *before* response begins, because it influences how the response will happen.
- Resources (personnel and financial) must be allocated to the response and recovery teams at a level appropriate to the severity of the incident.

4.2.1 Identification

The approach to the Identification Stage involves:

1) Validating the incident;
2) If an incident has occurred, identify its nature;
3) Classify the type of incident.

When a staff member notices a suspicious anomaly in data, a system, or the network, he or she begins this identification process.

4.2.1.1 Determine the Symptoms

Determining whether an anomaly is symptomatic of an incident is difficult since many symptoms of a security incident can also be something else entirely, (e.g., errors in system configuration, application bugs, hardware failures, user error, etc.).

Typical symptoms of computer security incidents include any or all of the following:

a) A system alarm or similar indication from an intrusion detection tool;
b) Suspicious entries in system or network accounting;
c) Accounting discrepancies;
d) Repeated unsuccessful logon attempts;
e) Unexplained new user accounts;
f) Unexplained new files or unfamiliar file names;
g) Unexplained modifications to file lengths and/or dates, especially in system executable files;
h) Unexplained attempts to write to system files or changes in system files;
i) Unexplained modification or deletion of data;
j) Denial/disruption of service or inability of one or more users to login to an account;
k) System crashes;
l) Poor system performance;
m) Operation of a program or sniffer device to capture network traffic;
n) Remote requests for information about systems or users (e.g., social engineering);
o) Unusual time of usage (many computer security incidents occur during non-working hours);
p) An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user;
q) Unusual usage patterns (e.g., programs are being compiled in the account of a user who does not know how to program, an escalation in disk usage by a single account);

4.2.1.2 Identify the Nature of the Incident

Although no single symptom conclusively shows that a computer security incident is taking place, observing one or more of these symptoms prompts the observer to investigate events more closely. System Administrators who encounter one or more of these symptoms should report it to the (*Security Team Name*). They will document, examine, and validate security incidents on a case by case basis.

4.2.1.3 Classification of Security Incidents

Although computer security incidents may take many forms and involve many devious means, there are certain types of attacks that occur more frequently than others.

4.2.1.3.1 Internal and External Threat

Internal Threat: An internal threat is any instance of a user misusing resources, running malicious code or attempting to gain unauthorized access to an application. Examples include unauthorized use of another user's account, unauthorized use of system privileges, and execution of malicious code that destroys data. More significant internal threats may include an otherwise authorized system administrator who performs unauthorized actions on a system.

External Threat: An external threat is any instance of an unauthorized person attempting to gain access to systems or cause a disruption of service. Examples include disruption/denial of service attacks, email spamming, and execution of malicious code that destroys data or corrupts a system.

4.2.1.3.2 Malicious Code Attacks

Malicious code is typically written to mask its presence thus it is often difficult to detect. Self-replicating malicious code, such as viruses and worms, can replicate so rapidly that containment can become an especially difficult problem. Dealing with malicious code attacks requires special considerations.

4.2.1.3.2.1 Virus Incidents

A virus is self-replicating code that operates and spreads by modifying executable files. Viruses are often user-initiated and would pose virtually no threat if every user always followed sound procedures. E-mail executables tend to carry infectious virus coding.

4.2.1.3.2.2 Macro Viruses

Macro viruses are a type of virus that utilizes an application's own macro programming language to distribute themselves (e.g., in MS Word or MS Excel).

4.2.1.3.2.3 Worms

A Worm is self-replicating code that is self-contained, (i.e., capable of operating without modifying any software). Worms are best noticed by looking at system processes. If an unfamiliar process (usually with an unknown name) is running and is consuming a large proportion of a system's processing capacity, the system may have been attacked using a worm. Worms also sometimes write unusual messages to users' displays to indicate their presence. Messages from unknown users that ask the user to copy an electronic mail message to a file may also propagate worms. Worms generally propagate themselves over networks and can spread very quickly.

4.2.1.3.2.4 Trojan Horses

Trojan horse programs are hostile programs masquerading as valid programs or utilities. Most malicious code is really a Trojan horse program in one way or another. Trojan horse programs are often designed to trick users into copying and executing them.

4.2.1.3.2.5 Cracking Utilities

Cracking utilities are programs sometimes planted in systems by attackers for a variety of purposes, such as elevating privileges, obtaining passwords, disguising the attackers' presence and so forth. They can be used from outside the system to gather information as well as to launch attacks against the target system.

4.2.1.3.3 Denial-Of-Service

Denial-of-service attacks attempt to push the limits of a device or system to the point where the device or system either fails or legitimate users are denied access.

4.2.1.3.4 Cracker Attacks

Crackers are users who attempt to obtain unauthorized access to remote systems. Most cracking attacks are automated and happen relatively quickly, which makes identifying and responding to them more difficult. Crackers now generally use "cracking utilities," (described above) which usually differ from conventional malicious code attacks in that most cracking utilities do not disrupt systems or destroy code. Cracking utilities are typically "a means to an end," such as obtaining administrative-level access, modifying audit logs, etc.

Indications that a cracker may have compromised a system include the following symptoms:

- Changes to directories and files;
- A displayed last time of login that was not the actual time of last login;
- Finding that someone else is logged into an individual's account from another terminal; and/or
- Inability to login to an account (often because someone has changed the password).

4.2.1.3.5 Technical Vulnerabilities

As opposed to an internal or external threat, a technical vulnerability is a "hole" or weakness in an information system or components (e.g., system security procedures, hardware design, and internal controls) that could be exploited to violate system security.

4.2.1.3.6 Legal Incidents

Legal incidents are not attacks directly against the organization or a vulnerability that can be exploited. They would include situations where local or federal law enforcement agents are involved. This may include, but is not limited to, agents entering a building with a warrant and confiscating hardware that has been involved in a security incident.

4.2.2 Incident Severity

Many security incidents, such as isolated occurrences of computer viruses, are easily handled via well-established procedures, and do not justify calling out the entire (*Security Team Name*). Below are the criteria used to classify the severity of security incidents, and which severities will result in (*Security Team Name*) activation.

Incidents are grouped into a few different severity levels, with broad sets of criteria for each level:

- ***Severity 1*** – Small numbers of system probes or scans detected on internal systems; isolated instances of known computer viruses easily handled by antivirus software.
- ***Severity 2*** – Small numbers of system probes or scans detected on external systems; intelligence received concerning threats to which systems may be vulnerable.
- ***Severity 3*** – Significant numbers of system probes or scans detected; penetration or denial of service attacks attempted with no impact on operations; widespread instances of known computer viruses easily handled by anti-virus software; isolated instances of a new computer virus not handled by anti-virus software.
- ***Severity 4*** – Penetration or denial of service attacks attempted with limited impact on operations; widespread instances of a new computer virus not handled by anti-virus software; some risk of negative financial or public relations impact.
- ***Severity 5*** – Successful penetration or denial of service attacks detected with significant impact on operations; significant risk of negative financial or public relations impact.

With the above criteria, incidents of Severity 3, 4, and 5 results in full (*Security Team Name*) activation, while incidents of Severity 1 and 2 are handled with minimal or no (*Security Team Name*) involvement.

4.2.3 Incident Declaration

When an incident requiring security team activation occurs, a formal incident is declared. Incident declaration is a procedure by which the security manager notifies management advisory board that an incident is taking place, and then assembles the other members of the (*Security Team Name*).

4.3 Response Phase

In the response phase, the (*Security Team Name*) gathers evidence (audit trails, log files, contents of files, etc.). If the "pursue" option was chosen, this process must be performed in a forensically sound manner so that the evidence will later be admissible in court; the team may need specialized technical assistance and advice from a third party to do this successfully.

Once evidence has been gathered, it is analyzed to determine the cause of the incident, the vulnerability or vulnerabilities being exploited, how to eliminate these vulnerabilities and/or stop the incident, and so forth. An assessment is also made of how far the incident has spread, (i.e., which systems are involved, and how badly have they been compromised).

4.3.1 Incident Evidence Handling

The collection, maintenance, and tracking of evidence is a critical step. This is especially true if the "pursue" option has been chosen.

4.3.1.1 Identify the Evidence

In order to protect the evidence, number, date and sign notes and printouts, store complete logs in a safe, or copy the entire log to an alternate location and secure appropriately.

4.3.1.2 Protect the Evidence

Documentation must be kept that indicates the sequence of individuals who have handled the evidence and the sequence of locations where the evidence has been stored. Dates and times *must* be specified as well. There *must not* be any lapses in time or date. The hand-off of evidence must be documented as well.

(*Security Team Name*) *must* obtain a backup of files on the system in which suspicious events have been observed as soon as a computer security-related incident has been declared.

Perpetrators of computer crimes are becoming increasingly proficient in quickly destroying evidence of their illegal activity, as such, be aware that, unless evidence is immediately captured by making a full backup, this evidence may be destroyed before it can be examined. This backup will provide a basis for comparison later to determine if any additional unauthorized activity has occurred.

4.3.2 Containment

The immediate objective for the containment stage is to limit the scope and magnitude of an incident as quickly as possible, rather than to allow the incident to continue in order to gain evidence for identifying and/or prosecuting the perpetrator.

The first critical decision to be made during the containment stage is what to do with critical information and/or computing services. A decision will be made regarding whether the sensitive data is to be left on the system or copied to media and taken off-line. Similarly, a decision may be made to move critical computing services to another system on another network where there is considerably less chance of interruption.

A decision on the operational status of the compromised system itself will be made. Whether this system should be:

1) Shutdown entirely;
2) Disconnected from the network, or;
3) Allowed to continue to run in its normal operational status

The reaction to an incident must be a measured response. The response must be dependent upon the level of criticality of the compromised components, not simply the system that was compromised. When an incident is discovered, there will be an initial risk assessment performed to evaluate the effect and impact of both the attack as well as the options to respond. That is, the responders are cautioned not to over react as overreaction has the potential of compromising the integrity, reliability, and safety of the system more than the incident itself.

4.3.2.1 Maintain a Low Profile

If a network-based attack is detected, care must be taken not to tip off the intruder. Avoid looking for the attacker with obvious methods - if hackers detect an attempt to locate them they may delete files and/or systems.

4.3.2.2 Back up the System

Back up the affected system to new, unused media if at all possible. Make a backup as soon as there are indications that a security incident has occurred. Making a full backup immediately captures evidence that may be destroyed before having a chance to look at it.

4.3.2.3 Change Passwords

It is recommended the system administrator and/or affected staff passwords be changed immediately on all affected systems. Passwords should be changed on compromised systems and on all systems that regularly interact with the compromised systems and notify all affected staff of the password change. If a sniffer device is detected or suspected, clear-text passwords may have been compromised on all systems on the LAN. In this case more accounts may be required to change their password.

4.3.3 Eradication

The next priority, after containing the damage from a computer security incident, is to remove the cause of the incident.

In the case of a virus incident, it will be removed from all systems and media by using one or more proven commercial virus eradication applications.

It is recognized that many intrusions leave benign or malignant artifacts that can be hard to locate. Therefore, (*Security Team Name*) will concentrate on the eradication of:

1) Malignant artifacts (e.g., Trojan horses) and;
2) Benign artifacts when they present a serious risk.

4.3.3.1 Determine the Cause and Symptoms

Use information gathered during the containment phase and collect additional information. If a single attack method cannot be determined list and rank the possibilities.

4.3.3.2 Improve Defenses

Implement appropriate protection techniques such as firewalls and/or router filters, moving the system to a new name/IP address, or in extreme cases, porting the machine's functions to a more secure operating system.

4.3.3.3 Malicious Code Attacks

Dealing with malicious code attacks requires special considerations.

4.3.3.3.1 Virus Incidents

Response: Provide all users with notices and alerts concerning viruses and the procedures that limit the spread of viruses. Ensure approved anti-virus tools are in place.

4.3.3.3.2 Macro Viruses

Response: Because macro viruses infect document files rather than programs, virus protection is extended to include the examination of all files using the latest commercial anti-virus application(s).

4.3.3.3.3 Worms

Response: If any staff member observes the symptoms of a worm, he or she must inform company management and/or (*Security Team Name*) immediately.
Prompt killing of any rogue processes created by the worm code will minimize the potential for damage. If the worm is a network-based worm (i.e., uses a network to spread itself), the workstation, server, client machine should be disconnected from the network

4.3.3.3.4 Trojan Horses

Response: If any staff member observes the symptoms of a Trojan horse, he or she must inform company management and/or (*Security Team Name*) immediately.

4.3.3.3.5 Cracking Utilities

Response: If a system is found to have cracking utilities on it, the response will vary depending on the circumstances. (*Security Team Name*) and/or company management must be informed immediately.

4.3.3.4 Denial-Of-Service (DOS)

Response: If a DOS attack is suspected the initial step is to identify the hosts under attack and begin filtering traffic directed at the targeted hosts. Sometimes this can be accomplished at the firewalls and routers under the control of the company, however, sometimes this may require coordination with upstream providers. The Internet2 resource center at the Research and Education Networking Information Sharing and Analysis Center (ren-isac@iu.edu, 317-278-6630) should be contacted to help speed the resolution of DOS attacks that originate from external sources. US-CERT may also be contacted to report the incident using their website at https://forms.us-cert.gov/report/

4.3.3.5 Cracker Attacks

Response: If these or other suspicious symptoms are noticed, (*Security Team Name*) and/or company management must be informed immediately.
If an attacker is caught in the act of obtaining unauthorized access, the (*Security Team Name*) follows procedures dependent on the nature of the attack.

- If the attacker has obtained administrative-level access, is deleting or changing user files, or has access to a machine that contains sensitive data, the attack poses a serious threat. In this case, (*Security Team Name*) locks the attacker out of this system by aborting the processes the attacker has created.
- If the cracker does not obtain administrative-level access and does not appear to be damaging or disrupting a system, (*Security Team Name*) may elect to allow the attacker to continue so as to collect the evidence necessary to determine any tools or vulnerabilities that need to be removed before serious damage occurs. To continue in this manner requires the approval of senior management.

A critical stage in cracker/hacker attacks is eradication. Because crackers so frequently use cracking utilities, it is important to ensure that no cracking scripts remain on the system once the cracker's attack has ceased. Ultimately, this often requires a complete re-imaging of any affected system.

Another critical component of responding to cracker/hacker attacks is handling evidence that is gathered. System log printouts, copies of malicious code discovered in systems, backup tapes, referring to chains of custody and entries recorded in logbooks may conceivably be used as evidence against perpetrators.

Response: If a system user finds evidence of such cracking artifacts, staff will notify (*Security Team Name*) immediately. (*Security Team Name*) will work to restore any file permissions and configuration settings that the attacker may have changed to their normal value. Resolving cracker/hacker attacks is risky, unless one possesses the technical skills, programs, and appropriate equipment.

4.3.3.6 Technical Vulnerabilities

Response: If a user discovers a technical vulnerability that could be used to subvert system or network security, he or she should immediately document that vulnerability. This documentation should record the following information:

(1) Vulnerability description;
(2) The circumstances under which the vulnerability was discovered;
(3) The specific impact of the weakness or design deficiency, and
(4) Indicate whether or not the applicable vendor has been notified.

After documenting the vulnerability, the information should be brought immediately to the attention of company management and/or (*Security Team Name*). Users *must not* send vulnerability reports over the network, or share vulnerability information with anyone outside of official channels. Company management and/or (*Security Team Name*) will coordinate the efforts to resolve the vulnerability with the system administrator and associated parties.

4.3.3.7 Legal Incidents

Response: Any time law enforcement agents are involved, a member of the company’s senior management team *must* be immediately notified. They will determine what legal actions to take. They will also decide when to get company’s Legal Counsel involved.

4.4 Recovery Phase

Recovery is defined as restoring a system to its normal mission status. The recovery phase begins once the response phase has been completed. There may at times be some overlap between these two phases. In this phase, the security team with the possibility of the security liaison restores the systems affected by the incident to normal operation. This may require reloading data from backup tapes, or reinstalling systems from their original distribution media. Once the affected systems have been restored, they are tested to make sure they are no longer vulnerable to the attack(s) that caused the incident. They are also tested to make sure they will function correctly when placed back into production.

4.4.1 Determine the Course of Action

In the case of relatively simple incidents (such as attempted but unsuccessful intrusions into systems), recovery requires only assurance that the incident did not adversely affect the company's computer or data resources.

In the case of complex incidents, such as malicious code planted by insiders, recovery may require a complete restoration operation from backup tapes, a re-image of the machine or partial/full implementation of the company's BCP plan in the event of a brute cyber terrorist attack.

4.4.2 Monitor and Validate System

First, determine the integrity of the backup itself by attempting to read its data. Once the system has been restored from backup, verify that the operation was successful and that system is back to its normal operating condition.

Second, run the system through its normal tasks monitoring it closely by a combination of network loggers and system log files. Monitor the system closely for potential "back doors" that may have escaped detection.

4.5 Maintenance Phase

The maintenance phase is also called "lessons learned." In this phase, the entire incident, as well as the response, are reviewed to determine which parts of the Security Incidence Response Plan worked correctly, and which parts need improvement. The areas in which improvement is needed are then corrected, and the Security Response Plan is updated accordingly. Other areas that need to be changed (policies, system configurations, etc.) may also be identified during this phase.

The (*Security Team Name*) realizes that devoting further resources to an incident after the Recovery Stage is not always cost effective. However, it also realizes that following up on an incident after Recovery helps to improve incident handling procedures.

4.5.1 Document Response Quality to Incident

The (*Security Team name*) will review every (x) months how well they responded to incidents:

- Was there sufficient preparation for the incident?
- Did detection occur promptly or, if not, why not?
- Could additional tools have helped the detection and eradication process?
- Was the incident sufficiently contained?
- Was communication adequate, or could it have been better?
- What practical difficulties were encountered?

4.5.2 Document Incident Costs

The (*Security Team name*) will review the staff time required to address incidents (including time necessary to restore systems). This leads to the following cost analysis:

- How much is the associated monetary cost?
- How much did the incident disrupt ongoing operations?
- Was any data irrecoverably lost, and, if so, what was the value of the data?
- Was any hardware damaged, and, if so, what was the cost?

Deriving a financial cost associated with an incident can help to justify future budget requests for security efforts.

4.5.3 Filing a Report

Depending on the type of incident, the (*Security Team Name*) will file a report of the incident to further staff awareness. Without endangering the company's security mechanisms, the report will be appropriately distributed.

4.5.4 Revising Policies and Procedures

Developing effective computer security policies and procedures often requires revising those efforts in light of experience. Therefore, lessons learned from each incident are used to review the computer security measures.

5 CONCLUSION

This security incident response plan provides reasonable methods for limiting the possibility of an adverse effect on all the company's computing assets and networks due to the occurrence of an information system security incident. It also provides reasonable methods for facilitating the rapid and successful recovery after an incident has occurred.

It stresses two fundamental principles related to incident response.

The first principle is the importance of following well-defined and systematic procedures for responding to computer security-related incidents. The five stages of the incident response procedures, Alert Phase, Triage Phase, Response Phase, Recovery Phase, and Maintenance Phase, provide a sound basis for securing all the company's computer resources. They also serve as a foundation for developing custom procedures tailored to specific operational environments. The only effective way to respond to incidents is to use a structured methodology.

The second principle is that unless conducted systematically, incident response efforts are of little value. Coordination of effort is a critical facet of incident response. The company's staff members can significantly reduce the staff hours needed to respond to incidents if properly coordinated.

Appendix C – Abbreviations and Acronyms

This section defines common abbreviations used in the natural gas pipeline, cyber security and control system industries.

ACC	Access Control Center [RFC 2828]
ACL	Access Control List [RFC 2828]
AES	Advanced Encryption Standard
AGA	American Gas Association
AIS	Automated Information System
ANSI	American National Standards Institute
API	American Petroleum Institute
CC	Common Criteria [ISO/IEC 15408]
CIDX	Chemical Industry Data Exchange
CERT	Computer Emergency Response Team
CGI	Common Gateway Interface
CIP®	Common Industrial Protocol (formerly Control and Information Protocol)
CMVP	Cryptographic Module Validation Program
COM	Component Object Model
COOP	Continuity of Operation Plan
COTS	Commercial Off The Shelf
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check [RFC 2828]
CSP	Corporate Security Program
DAC	Discretionary Access Control
DCOM	Distributed Component Object Model
DCS	Distributed Control System
DDoS	Distributed Denial-of-Service
DEK	Data Encryption Key [RFC 2828]
DES	Digital Encryption Standard
DHS	United States Department of Homeland Security
DLL	Data Link Layer [ISO/IEC 7498-1]
DMZ	Demilitarized Zone
DoS	Denial-of-Service
DOT	U.S. Department of Transportation
EMI	Electro-Magnetic Interference
EFM	Electronic Flow Measurement
ERP	Enterprise Resource Planning
ESD	Emergency Shutdown
FAL	Fieldbus Application Layer [IEC 61158-5]
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GPS	Global Positioning System

GUI	Graphical User Interface
HIDS	Host Intrusion Detection System
HMI	Human Machine Interface
HSAS	Homeland Security Advisory System
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
ICMP	Internet Control Message Protocol
ICS	Industrial Control System
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Devices
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
INGAA	Interstate Natural Gas Association of America
IP	Intellectual Property
IP	Internet Protocol
IPS	Intrusion Prevension System
IPsec	Internet Protocol Security
ISA	The International Society of Automation
IT	Information Technology
KEK	Key Encryption Key [RFC 2828]
LAN	Local Area Network
LOPA	Layer of Protection Analysis
MAC	Media Access Control
MTU	Master Terminal Unit
NAT	Network Address Translation
NFAT	Network Forensics and Analysis Tool
NIC	Network Interface Card
NIDS	Network Intrusion Detection System
NIST	U.S. National Institute of Standards and Technology
NSA	National Security Administration
OEM	Original Equipment Manufacturer
OLE®	Object Linking and Embedding
OPC®	OLE for Process Control
OS	Operating System
OSI/RM	Open Systems Interconnect Reference Model
PAP®	Password Authentication Protocol
PCS	Process Control System
PCN	Process Control Network
PDA	Personal Digital Assistant
PDU	Protocol Data Unit [ISO/IEC 7498-1]
PGP®	Pretty Good Privacy®
PHA	Process Hazard Analysis

PHMSA	Pipeline and Hazardous Materials Safety Administration
PIMS	Process Information Management System
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PPP	Point-to-Point Protocol
PSM	Process Safety Mangement
PRNG	Pseudorandom Number Generator
RBAC	Role-Based Access Control
RFC	Request For Comment
RFP	Request For Proposal
ROM	Read-Only Memory
RRAS	Routing and Remote Access Service
RSA®	Rivest, Shamir and Adleman
RTOS	Real-time Operating System
RTU	Remote Terminal Unit
SAM	Security Accounts Manager
SANS	SysAdmin, Audit, Network, Security Institute
SCADA	Supervisory Control and Data Acquisition
SDU	Service Data Unit [ISO/IEC 7498-1]
SIL	Safety IntegrityLevel
SIF	Safety Instrumented Function
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign On
SVA	Security Vulnerability Assessment
TCP	Transmission Control Protocol
TLS	Transport Layer Security
ToE	Targets of Evaluation
TSA	Transportation Security Administration
UDP	User Datagram Protocol
USB	Universal Serial Bus
VDS	Virus Detection System
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network
XML	Extensible Markup Language

Appendix D – Common Terms and Definitions

This section lists the terms, definitions and abbreviations used in this document.

Most definitions have been taken from established industry sources. Cited sources include:

[1] CNSS Instruction No. 4009, National Information Assurance Glossary, May 2003, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

[2] SANS Glossary of Terms used in Security and Intrusion Detection, May 2003, http://www.sans.org/resources/glossary.php

[3] RFC 2828, Internet Security Glossary, May 2000

[4] Federal Information Processing Standards (FIPS) PUB 140-2, (2001) "SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES," Section 2, Glossary of Terms and Acronyms, U.S. National Institute of Standards and Technology.

[5] ISO/IEC 7498: Information processing systems – Open System Interconnection – Basic reference Model, Part 2: Security Architecture

[6] Federal Information Processing Standards Publication, FIPS PUB 140-2, Security Requirements for Cryptographic Modules, December 2002

The following terms have been identified.

- **Anomaly**: An unusual or atypical event (in a system or network).
- **Attack Scanner:** A tool used to remotely connect to systems and determine security vulnerabilities that have not been fixed.
- **Audit**: An independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [1]
- **Audit Service**: Security service that records information needed to establish accountability for system events and for the actions of system entities that cause them. [3]
- **Authenticate**: To verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an IS, or to establish the validity of a transmission. [1]
- **Authentication**: A security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [1]
- **Authorization**: A right or a permission that is granted to a system entity to access a system resource. [3]
- **Authorization Process**: A procedure for granting authorization rights. [3]
- **Automated information system** (AIS): An organized assembly of resources and procedures--i.e., computing and communications equipment and services, with their supporting facilities and personnel - that collect, record, process, store, transport, retrieve, or display information to accomplish a specified set of functions. [3]

INGAA Proprietary, Confidential, and Sensitive Security Information (SSI)

- **Automation Cell (AC):** A zone within a larger zone within a plant, used to partition a large plant into separate major areas with independent production missions.
- **Availability:** The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system; i.e., a system is available if it provides services according to the system design whenever users request them. [3]
- **Bandwidth:** Commonly used to mean the capacity of a communication channel to pass data through the channel in a given amount of time. usually expressed in bits per second. [3]
- **Black channel:** Communication channel without available evidence of design or validation according to IEC 61508 and IEC WD/61784-3.
- **Boundary:** A software, hardware, or physical barrier that limits access to a system or part of a system. [1]
- **British Standard 7799:** Part 1 is a standard code of practice and provides guidance on how to secure an information system. Part 2 specifies the management framework, objectives, and control requirements for information security management systems [B7799]. The certification scheme works like ISO 9000. It is in use in the UK, the Netherlands, Australia, and New Zealand and might be proposed as an ISO standard or adapted to be part of the Common Criteria.
- **Certificate:** See "digital certificate".
- **Certification Authority:** An entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate. [3]
- **Cipher:** A cryptographic algorithm used for encryption and decryption. [3]
- **Ciphertext:** Data that has been transformed by encryption so that its semantic information content (i.e., its meaning) is no longer intelligible or directly available. [3]
- **Cleartext:** Data in which the semantic information content (i.e., the meaning) is intelligible or is directly available. [3]
- **Client:** A device or application receiving or requesting services or information from a server application. [4]
- **Client-side Policy Enforcement:** A technological means to ensure that a remote client, before being given access to a server network, is in accordance with policies imposed by the server network zone.

  NOTE: Such policies could refer to installation/update/status of virus checkers, installation/update/status of host based intrusion detection systems, configuration settings, user accounts, restrictions on concurrent network connections, or installed applications. This functionality has different names depending on the vendors. One common designator for the underlying concept is the "client quarantine".
- **Common Criteria for Information Technology Security:** The Common Criteria is a standard for evaluating information technology products and systems, such as operating systems, computer networks, distributed systems, and applications. It states requirements for security functions and for assurance measures. [3]

- **Communication Channel:** A logical connection between two or more end-points within a communication system.
- **Communication Path:** A logical connection between a source and one or more destinations, which could be devices, physical processes, data items, commands or programmatic interfaces.

  NOTE: The communication path is not limited to wired or wireless networks, but includes other means of communication such as memory, procedure calls, state of physical plant, portable media, human interactions etc.
- **Communication Security (ComSec):** Communication security is:
  - A measure(s) that implement and assure security services in a communication system, particularly those that provide data confidentiality and data integrity and that authenticate communicating entities;
  - A state that is reached by applying security services, in particular, state of data confidentiality, integrity, and successfully authenticated communications entities. [3]

  NOTE: This phrase is usually understood to include cryptographic algorithms and key management methods and processes, devices that implement them, and the life cycle management of keying material and devices.
- **Communication Security Layer:** Communication layer that includes all the necessary measures to provide secure transmission of data in accordance with specific requirements.
- **Communication System:** An arrangement of hardware, software and propagation media to allow the transfer of messages (ISO/IEC 7498 application layer service data units) from one application to another.
- **Compromise:** The unauthorized disclosure, modification, substitution, or use of sensitive data (including plaintext cryptographic keys and other critical security parameters). [6]
- **Computer Security:** Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated. [1]
- **Confidentiality:** Assurance that information is not disclosed to unauthorized individuals, processes, or devices. [1]
- **Contingency Plan:** A plan for emergency response, backup operations, and post-disaster recovery in a system as part of a security program to ensure availability of critical system resources and facilitate continuity of operations in a crisis. [3]
- **Control Network (CN):** Those networks of an enterprise that are the subject to this standard, typically connected to equipment that controls physical processes and that is time or safety critical.

  NOTE: The CN can be subdivided into zones, and there can be multiple separate CNs within one enterprise and site.

- **Controlled Space:** Three-dimensional space surrounding system equipment, within which unauthorized individuals are denied unrestricted access and are either escorted by authorized individuals or are under continuous physical or electronic surveillance. [1]
- **Cost:** Value impact to the organization or person that can be measured.
- **Countermeasure:** An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken. [3]
- **Cracker**: Someone who tries to break the security of, and gain access to, someone else's system without being invited to do so (See: Hacker and Intruder). [3]
- **Checksum**: Value computed, via some parity or hashing algorithm, on information requiring protection against error or manipulation.
- **Cracking Utilities**: Programs planted in systems by attackers for a variety of purposes such as elevating privileges, obtaining passwords, and disguising the attacker's presence.
- **Credentials:** Data that is transferred or presented to establish either a claimed identity of an entity. [3]
- **Critical:** A condition of a service or other system resource such that denial of access to (i.e., lack of availability of) that resource would jeopardize a system user's ability to perform a primary function or would result in other serious consequences. [3]
- **Critical Security Parameter (CSP):** Security-related information (e.g., secret and private cryptographic keys, and authentication data such as passwords and PINs) whose disclosure or modification can compromise the security of a cryptographic module. [6]
- **Cryptanalysis:** The mathematical science that deals with analysis of a cryptographic system in order to gain knowledge needed to break or circumvent the protection that the system is designed to provide. [3]
- **Cryptographic Algorithm:** An algorithm that is based upon the science of cryptography, including encryption algorithms, cryptographic hash algorithms, digital signature algorithms, and key agreement algorithms. [3]

- **Cryptographic Key**: Either:
    - (Usually shortened to just "key") An input parameter that varies the transformation performed by a cryptographic algorithm, [3] or
    - A parameter used in conjunction with a cryptographic algorithm that determines:
        - The transformation of plaintext data into ciphertext data;
        - The transformation of ciphertext data into plaintext data;
        - A digital signature computed from data;
        - The verification of a digital signature computed from data;
        - An authentication code computed from data;
        - An exchange agreement of a shared secret. [4]
- **Cyber attack:** Exploitation of the software or firmware vulnerabilities of information technology-based control components.
- **Cyclic Redundancy Check (CRC):** A type of checksum algorithm that is not a cryptographic hash but is used to implement data integrity service where accidental changes to data are expected. [3]
- **Data Compromise:** A security incident in which information is exposed to potential unauthorized access, such that unauthorized disclosure, alteration, or use of the information may have occurred. [3]
- **Data Encryption Key (DEK):** A cryptographic key that is used to encipher application data. [3]
- **Data Integrity:** Property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner. [3]

  NOTE: This term deals with constancy of and confidence in data values, not with the information that the values represent (see: correctness integrity) or the trustworthiness of the source of the values (see: source integrity).
- **Data Link Layer Protocols:** Protocols for interpreting electrical signals as data, error checking, physical addressing and media access control. [2]
- **Decryption:** The process of changing ciphertext into plaintext using a cryptographic algorithm and key. [3]
- **Defense in Depth:** A security architecture based on the idea that any one point of protection may, and probably will, be defeated. It implies layers of security and detection, even on single systems and provides the following features:
    - Attackers are tasked with breaking through or bypassing each layer without being detected;
    - A flaw in one layer can be mitigated by capabilities in other layers;
    - System security becomes a set of layers within the overall network security;
    - Security is improved by requiring the attacker to be perfect while ignorant.
- **Demilitarized Zone (DMZ):** A perimeter network segment that is logically located between internal and external networks. It purpose is to enforce the internal network's policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks. [1]

- **Denial of Service (DOS):** The prevention or interruption of authorized access to a system resource or the delaying of system operations and functions. [3]
- **Digital Certificate:** A certificate document in the form of a digital data object (a data object used by a computer) to which is appended a computed digital signature value that depends on the data object. [3]
- **Digital Signature:** A value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity. [3]
- **Distributed Control System (DCS):** Type of control system in which the system elements are dispersed but operated in a coupled manner, generally with coupling time constants much shorter than those found in SCADA systems.

  NOTE: Digital control systems are commonly associated with continuous processes such as electric power generation; oil and gas refining; chemical, pharmaceutical and paper manufacture, as well as discrete processes such as automobile and other goods manufacture, packaging, warehousing, etc.
- **Domain:** An environment or context that is defined by a security policy, security model, or security architecture to include a set of system resources and the set of system entities that have the right to access the resources. [3]
- **Domain Authentication Server:** A server that stores and manages user accounts and credentials for the users of the associated network domain.
- **Domain Name System (DNS):** The main Internet operations database, which is distributed over a collection of servers and used by client software for purposes such as translating a domain name-style host name into an IP address (e.g., "rosslyn.bbn.com" is "192.1.7.10") and locating a host that accepts mail for some mailbox address. [3]
- **Dual Control:** A procedure that uses two or more entities (usually persons) operating in concert to protect a system resource, such that no single entity acting alone can access that resource. [3]

  NOTE: dual control provides a countermeasure to attacks by a single disgruntled, subverted or coerced insider.
- **Electronic Security:** Comprises the concepts of identification, authentication, accountability, authorization, availability and privacy. The objective is to preclude unauthorized use, modifications to, disclosure, loss of revenue or destruction of critical systems or informational assets in an effort to reduce the risk of personal injury or possibility of endangering public health, loss of public or consumer confidence, disclosure of sensitive assets, and protection of business assets. These concepts are applied to any system in the production process and include both standalone and networked components. Communications between systems may be either through internal messaging or by any human or machine interfaces that authenticate, operate, control, or exchange data with any of these control systems.

- **Encryption:** A cryptographic transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called "decryption", which is a transformation that restores encrypted data to its original state. [3]
- **Evaluated System:** Refers to a system that has been evaluated against security criteria such as the TCSEC or the Common Criteria. [3]
- **External Device (ED):** All devices that can contain computer programs or data except for those of the protected industrial automation plant.
- **External Network (EN):** All networks except for the (possibly distributed) Control Network.
- **Fail Safe:** Automatic protection of programs and/or processing systems when hardware or software failure is detected. [1]
- **Fieldbus Network:** Communication system used in industrial automation or process control applications.

  NOTE: This concept is further detailed in [IEC 61158] and [IEC 61784-1].
- **Filtering Router:** An internetwork router that selectively prevents the passage of data packets according to a security policy. [3]
- **Firewall:** An inter-network gateway that restricts data communication traffic to and/or from one of the connected networks (the one said to be "inside" the firewall) and thus protects that network's system resources against threats from the other network (the one that is said to be "outside" the firewall). [3]

  NOTE: A firewall may be either an application installed on a general-purpose computer or a dedicated, potentially proprietary platform (appliance), that forwards or rejects/drops packets on a network. Typically firewalls are used to define zone borders.
- **Firewall Host:** A general-purpose computer or dedicated proprietary platform on which a firewall application runs.
- **Flooding:** An attack that attempts to cause a failure in (specifically, in the security of) a computer system or other data processing entity by providing more input than the entity can process properly. [3]
- **Gateway:** A relay mechanism that attaches to two (or more) computer networks that have similar functions but dissimilar implementations and that enables host computers on one network to communicate with hosts on the other; an intermediate system that is the interface between two computer networks. [3]
- **Hacker:** Someone with a strong interest in computers, who enjoys learning about them and experimenting with them. [3]

  This recommended definition is the original meaning of the term (circa 1960), which then had a neutral or positive connotation of "someone who figures things out and makes something cool happen". Today, the term is frequently misused, especially by journalists, to have the pejorative meaning of cracker (See: cracker). [3]

- **Hash Function:** An algorithm that computes a value based on a data object (such as a message or file; usually variable-length; possibly very large), thereby mapping the data object to a smaller data object (the "hash result") which is usually a fixed-size value.

  NOTE: The kind of hash function needed for security applications is called a "cryptographic hash function", an algorithm for which it is computationally infeasible (because no attack is significantly more efficient than brute force) to find either (a) a data object that maps to a pre-specified hash result (the "one-way" property) or (b) two data objects that map to the same hash result (the "collision-free" property).

- **Host:** A computer that is attached to a communication sub-network or internet-work and can use services provided by the network to exchange data with other attached systems. [3]
- **Host-Based Intrusion Detection System (HIDS):** An application that detects attacker activity on a host from characteristics such as change of files (file system integrity checker), operating system call profiles, etc. (See "intrusion detection").
- **INFOSEC:** An abbreviation for "information security", referring to security measures that implement and assure security services in computer systems (i.e., COMPUSEC) and communication systems (i.e., COMSEC). [3]
- **Integrity:** The quality of a system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. [1]

  NOTE: In a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

- **Interception:** The capture and disclosure of message contents; often referred to as sniffing, or use of traffic analysis to compromise the confidentiality of a communication system based on message destination or origin, frequency or length of transmission, and other communication attributes.
- **Interface:** A logical entry or exit point of a cryptographic module that provides access to the module for logical information flows representing physical signals. [4]
- **Intranet:** Computer network, especially one based on Internet technology, that an organization uses for its own internal, and usually private, purposes and that is closed to outsiders. [3]
- **Intruder:** An entity that gains or attempts to gain access to a system or system resource without having authorization to do so (See: cracker).
- **Intrusion:** The unauthorized act of bypassing the security mechanisms of a system. [1]
- **Intrusion Detection:** A security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner. [3]
- **IP Address:** Inter-network address of a computer that is assigned for use by the Internet Protocol and other protocols. [3]

- **Key Center:** A centralized key distribution process (used in cryptography), usually a separate computer system, that uses key-encrypting keys (master keys) to encrypt and distribute session keys needed in a community of users. [3]
- **Key Distribution**: Either:
  - The transport of a key and other keying material from an entity that either owns the key or generates the key to another entity that is intended to use the key, [3] or:
  - Process that delivers a cryptographic key from the location where it is generated to the locations where it is used in a cryptographic algorithm. [3]
- **Key Encapsulation:** A key hiding technique for storing knowledge of a cryptographic key by encrypting it with another key and ensuring that only certain third parties called "recovery agents" can perform the decryption operation to retrieve the stored key. [3]
- **Key Encrypting Key (KEK):** A Cryptographic key that is used to encrypt other keys, either DEKs or other KEKs, but usually is not used to encrypt application data. [3]
- **Key Escrow:** Key recovery technique, such as key escrow or key encapsulation, for storing knowledge of a cryptographic key or parts thereof in the custody of one or more third parties called "escrow agents", so that the key can be recovered and used in specified circumstances. [3]
- **Key Establishment:** Process that combines the key generation and key distribution steps needed to set up or install a secure communication association. [3]
- **Key Generation:** Process that creates the sequence of symbols that comprise a cryptographic key. [3]
- **Key Length:** Number of bits needed to be able to represent any of the possible values of a cryptographic key. [3]
- **Key Management:** process of handling and controlling cryptographic keys and related material (such as initialization values) during their life cycle in a cryptographic system, including ordering, generating, distributing, storing, loading, escrowing, archiving, auditing, and destroying the keys and related material. [3]
- **Key Pair:** A public key and its corresponding private key used with a public key algorithm. [3]
- **Key Recovery:** techniques that provide an intentional, alternate (i.e., secondary) means to access the key used for data confidentiality service in an encrypted association. [3]
- **Key Transport:** Key establishment method by which a secret key is generated by one entity in a communication association and securely sent to another entity in the association. [3]
- **Keyed Hash:** A cryptographic hash in which the mapping to a hash result is varied by a second input parameter that is a cryptographic key. [3]
- **Local Area Network (LAN):** A communications network designed to connect computers and other intelligent devices in a limited geographic area (typically under 10 km). [2]

- **Latency:** The time interval between when a message is sent by one device and received by a second device.
- **Least Privilege:** Principle that a security architecture should be designed so that each system entity is granted the minimum system resources and authorizations that the entity needs to do its work.
- **Manufacturing And Control Systems:** Includes all systems (personnel, hardware, and software) that can affect or influence the safe, secure and reliable operation of an industrial process. They include, but are not limited to:
  - Process control systems, including Distributed Control Systems (DCS), Programmable Logic Controllers (PLC), Remote Terminal Units (RTU), Intelligent Electronic Devices (IED), Supervisory Control and Data Acquisition (SCADA), networked electronic sensing and control, and monitoring and diagnostic systems (In this context, process control systems include Basic Process Control System (BPCS) and Safety Instrumented System (SIS) functions, whether they are physically separate or integrated;
  - Associated information systems such as advanced or multi-variable control, online optimizers, dedicated equipment monitors, graphical interfaces, process historians, manufacturing execution systems and plant information management systems;
  - Associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes.
- **Malicious code attacks**: Attacks by programs such as viruses, Trojan horses, worms, and scripts used by crackers/hackers to gain privileges, capture passwords, and/or modify audit logs to exclude unauthorized activity.
- **Malicious Logic:** Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose. [1]
- **Malware:** A contraction of "malicious software". (See: "malicious logic")
- **Man-In-The-Middle:** Form of active attack in which the attacker intercepts and selectively modifies communicated data in order to masquerade as one or more of the entities involved in a communication association. [3]
- **Manufacturing Operations:** Manufacturing operations encompass the collection of production, maintenance, and quality assurance operations with other activities of a production facility, including:
  - Manufacturing or processing facility activities that coordinate the personnel, equipment, and material involved in the conversion of raw materials and/or parts into products;
  - Functions that may be performed by physical equipment, human effort, and information systems;
  - Managing information about the schedules, use, capability, definition, history, and status of all resources (personnel, equipment, and material) within the manufacturing facility.

- **Masquerade Attack:** A type of attack in which one system entity illegitimately assumes the identity of another entity. [3]
- **Network-Based Intrusion Detection System (NIDS):** An application that reads all packets, not just those sent to it, from a network and detects potentially malicious packets based on rules or algorithms (See: "intrusion detection"). **Network Layer Protocol:** Protocols for routing of messages through a complex network. Layer 3 of the OSI reference model. [2]
- **Non-Repudiation:** A security service that provides protection against false denial of involvement in a communication. [3]
- **Out Of Band:** Transfer of information using a channel that is outside (i.e., separate from) the channel that is normally used. [3]

  NOTE: Out-of-band mechanisms are often used to distribute shared secrets (e.g., a symmetric key) or other sensitive information items (e.g., a root key) that are needed to initialize or otherwise enable the operation of cryptography or other security mechanisms.
- **Password:** A secret data value, usually a character string, that is used as authentication information. [3]
- **Penetration:** Successful, repeatable, unauthorized access to a protected system resource. [3]
- **Personal Identification Number (PIN)**: An alphanumeric code or password used to authenticate an identity. [4]
- **Physical Layer Protocol:** Protocols for transmitting raw electrical signals over the communications channel. Deals with transmission physics such as cabling, modulation, and transmission rates. Layer 1 of the OSI reference model. [2]
- **Plaintext:** Data that are input to and transformed by an encryption process, or that are output by a decryption process. [3]
- **Point-To-Point Protocol (PPP):** The protocol defined in RFC 1661, the Internet standard for transmitting network layer datagrams (e.g. IP packets) over serial point-to-point links.
- **Private Key:** Secret component of a pair of cryptographic keys used for asymmetric cryptography. [3]
- **Privilege:** An authorization or set of authorizations to perform security relevant functions, especially in the context of a computer operating system. [3]
- **Production Traffic:** Communications exchanged between the CN and external users in order to facilitate the intended operation of the systems, e.g. physical plant status, production orders, control programs, etc, including configuration, test, and maintenance of control related devices, but not security related devices.

  NOTE: The intent is to include all communications associated with normal plant operation, but to exclude all communications related solely to IT and security infrastructure management, e.g. firewall configuration, log messages, authentication exchanges, etc. Production traffic is the reason why there is an interconnection between the CN and other networks.

- **Protection Profile:** An implementation-independent set of security requirements for a category of Targets of Evaluation (TOEs) that meet specific consumer needs. [4,6]
- **Protocol:** Set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems. [3]
- **Proxy Server:** Computer process – often used as, or as part of, a firewall – that relays a protocol between client and server computer systems, by appearing to the client to be the server and appearing to the server to be the client. [3]
- **Proxy Gateway:** Gateway that terminates an incoming connection and opens a new connection to the destination on the same or a different network interface to pass on the traffic.

  NOTE: Because a new connection is made from the proxy to the destination, the destination is protected against any layer 3 and layer 4 malformed packets from external sources. Mostly, proxies copy data between their interfaces without further inspection, which does not prevent application level attacks or protocol tunneling. Some proxy firewalls actually evaluate the traffic for some protocols. This may be, in contrast to stateful inspection, not only done by pattern matching on the payload, but by actually processing the content.

- **Pseudo-Random:** Sequence of values that appears to be random (i.e., unpredictable) but is actually generated by a deterministic algorithm. [3]
- **Pseudorandom Number Generator (PRNG):** An algorithm that produces a sequence of bits that are uniquely determined from an initial value called a seed. The output of the PRNG "appears" to be random, i.e., the output is statistically indistinguishable from random values. A cryptographic PRNG has the additional property that the output is unpredictable, given that the seed is not known. [3]
- **Public Key:** Publicly-disclosable component of a pair of cryptographic keys used for asymmetric cryptography.
- **Public Key Certificate:** A set of data that uniquely identifies an entity, contains the entity's public key, and is digitally signed by a trusted party, thereby binding the public key to the entity. [4]
- **Public Key (Asymmetric) Cryptographic Algorithm:** A cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that deriving the private key from the public key is computationally infeasible. [4]
- **Public Key Infrastructure (PKI):** A framework that is established to issue, maintain, and revoke public key certificates. [3]
- **Random:** (security usage) unpredictable and "unguessable". [3]
- **Redundancy:** Existence of means, in addition to the means which would be sufficient for a functional unit to perform a required function or for data to represent information

  NOTE 1: Redundancy is used primarily to improve reliability or availability.

- **Reflection Attack**: Type of replay attack in which transmitted data is sent back to its originator. [3]

- **Rekey**: Change the value of a cryptographic key that is being used in an application of a cryptographic system. [3]
- **Reliability**: Ability of a system to perform a required function under stated conditions for a specified period of time. [3]
- **Remote Access Workplace**: Host on which actual applications execute (e.g., a Control Network user interface), which is mirrored via a remote access protocol to a remote access client.

  NOTE: This can also be used by staff in the plant to monitor locally the activities conducted from the remote client, or vice versa. There could be multiple remote access workplaces in a Control Network.
- **Remote Client (RC)**: Host outside the control network that is temporarily or permanently connected to the control network via a communication link in order to directly or indirectly interactively access parts of the control equipment on the Control Network.
- **Replay Attack**: An attack in which a valid data transmission is maliciously or fraudulently repeated, either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack. [3]
- **Repudiation**: Denial by a system entity that was involved in an association (especially an association that transfers information) of having participated in the relationship (See: accountability, non-repudiation service). [5]
- **Residual Risk:** The remaining risk after the security controls have been applied. [1]
- **Risk:** An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result. [3]
- **Risk Analysis, Risk Assessment:** The process that systematically identifies valuable system resources and threats to those resources, quantifies loss exposures (i.e., loss potential) based on estimated frequencies and costs of occurrence, and (optionally) recommends how to allocate resources to countermeasures so as to minimize total exposure.
- **Risk Management:** The process of identifying and applying countermeasures commensurate with the value of the assets protected based on a risk assessment. [1]
- **Role-Based Access Control (RBAC):** Form of identity-based access control where the system entities that are identified and controlled are functional positions in an organization or process [3]
- **Router:** A computer that is a gateway between two networks at OSI layer 3 and that relays and directs data packets through that internetwork. The most common form of router operates on Internet Protocol (IP) packets [3]
- **Rule-Based Security Policy:** Security policy based on global rules imposed for all users. These rules usually rely on comparison of the sensitivity of the resource being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users [5]
- **Safety:** A property of a system being free from risk of causing harm to system entities and outside entities. [3]

- **Secret:** A condition of information being protected from being known by any system entities except those who are intended to know it. [3]
- **Secretkey:** A cryptographic key, used with a secret key cryptographic algorithm that is uniquely associated with one or more entities and should not be made public. [4]
- **Secret Key (Symmetric) Cryptographic Algorithm:** A cryptographic algorithm that uses a single secret key for both encryption and decryption. [4]
- **Security Architecture:** A plan and set of principles that describe the security services that a system is required to provide to meet the needs of its users, including:
  - The system elements required to implement the services, and
  - The performance levels required in the elements to deal with the threat environment. [3]
- **Security Audit:** an independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures. [5]
- **Security Audit Trail:** a chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event in a security-relevant transaction from inception to final results. [3]
- **Security Components: (also called Security Countermeasures):** techniques such as firewalls, authentication modules, or encryption software used to improve the security performance of the manufacturing and control system.
- **Security Domain:** An environment or context that is defined by a security policy, security model, or security architecture to include a set of system resources and the set of system entities that have the right to access the resources.
- **Security Event:** An occurrence in a system that is relevant to the security of the system. [3]
- **Security Function:** A function implemented by a security-related system, intended to achieve or maintain a secure state for the system with respect to a specific category of threat.
- **Security Gateway:** A gateway that separates trusted (or relatively more trusted) hosts on the internal network side from untrusted (or less trusted) hosts on the external network side. [3]
- **Security Incident:** Security event that involves a security violation. [3]
- **Security Intrusion:** Security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system (or system resource) without having authorization to do so. [3]
- **Security Level (SRL) :** Hierarchical classification of security functions and processes that provide resistance to attack.
- **Security Management Infrastructure:** System elements and activities that support security policy by monitoring and controlling security services and mechanisms, distributing security information, and reporting security events. [5]

- **Security Management Network (SMN):** A network that is dedicated to administrating a set of security device, where each of those devices is connected to the SMN via a dedicated network interface, such that no production traffic flows through the SMN so that the SMN realizes out-of-band management of the connected security mechanisms.
- **Security Measure:** Measure against possible security attacks on a communication system.
- **Security Perimeter:** Boundary of the domain in which a security policy or security architecture applies; i.e., the boundary of the space in which security services protect system resources. [3]
- **Security Performance:** Security performance may be evaluated in terms of a program's compliance, completeness of measures to provide specific threat protection, post compromise analysis, review of changing business requirements, new threat and vulnerability information, and periodic audit of control systems to ensure that security measures remain effective and appropriate. Tests, audits, tools, measures, or other methods are required to evaluate security practice performance.
- **Security Policy:** A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources. [3]
- **Security Practices:** Procedures that provide a means of capturing experiences and activities that help ensure system protection and reduce potential systems compromise. Subject areas include physical security, procedures, organization, design, and programming. Security practices include the actual steps to be taken to ensure system protection.
- **Security Procedures:** Practices that define exactly how practices are implemented and executed. They are implemented through personnel training and actions using currently available and installed technology (such as disconnecting modems). Procedures and contained criteria also include more technology-dependent system requirements that need careful analysis, design, planning, and coordinated installation and implementation.
- **Security Program:** A policy or procedure that brings together all aspects of managing security, ranging from the definition and communication of policies through implementation of best industry practices and ongoing operation and auditing.
- **Security Services:** mechanisms used to provide confidentiality, data integrity, authentication or non-repudiation of information. [3]
- **Security Violation:** An act or event that violates or otherwise breaches security policy.
- **Separation Of Duties:** The practice of dividing the steps in a system function among different individuals, so as to keep a single individual from subverting the process (See: Dual Control).
- **Server:** A device or application that provides information or services to client applications and devices. [3]
- **Sniffer**: A device or program that captures packets transmitted over a network.

- **Sniffing:** See Interception.
- **Social engineering**: The act of manipulating people into performing actions or divulging confidential information, rather than breaking in or using technical hacking techniques.
- **Split Knowledge:** A security technique in which two or more entities separately hold data items that individually convey no knowledge of the information that results from combining the items (See: Dual Control).
- **Spoof:** Pretending to be an authorized user and performing an unauthorized action. [3]
- **Static Filtering Firewall:** A firewall that bases its forwarding decisions between its two or more network interfaces on rules that inspect ISO/OSI layer 3 and layer 4 information without keeping state information.

  Note: This type of filtering is often available in low-end routers and modems.
- **Stateful Filtering Firewall:** A firewall that bases its forwarding decisions between its two or more network interfaces on rules that inspect ISO/OSI layer 3 and layer 4 information and associated session / conversation state information, permitting determination of whether certain incoming data are unsolicited or in response to a previous outgoing request.

  Note: This type of functionality is typically available with mid-range routers as well as dedicated firewalls.
- **Stateful Inspection Firewall:** An enhanced stateful filtering firewall that bases its forwarding decisions between its two or more network interfaces on rules that inspect ISO/OSI layer 3, layer 4 and application layer information to determine whether the data stream corresponds to expectations for the application.

  NOTE: Stateful inspection firewalls can be used to securely filter protocols with complex port behavior (e.g. FTP) or to determine whether a port is used to tunnel data belonging to an unexpected application. Such firewalls are limited to a small product-specific set of application protocols. For other protocols these firewalls typically rely on stateful filtering.
- **Supervisory Control And Data Acquisition (SCADA) System:** A type of loosely-coupled distributed monitoring and control system commonly associated with electric power transmission and distribution systems, oil and gas pipelines, and water and sewage systems.
- **Survivability:** The ability of a system to remain in operation or existence despite adverse conditions, including natural occurrences, accidental actions, and attacks on the system.
- **Symmetric Cryptography:** A branch of cryptography involving algorithms that use the same key for two complementary steps of the algorithm. [5]
- **Symmetric Key:** A single cryptographic key that is used with a secret (symmetric) key algorithm. [3]
- **Symmetric Key Algorithm:** See Secret Key Cryptographic Algorithm. [3]

- **System Owner / Operator:** The business enterprise responsible for operating a DCS or SCADA system.
- **System Security Officer:** Person responsible for enforcement or administration of the security policy that applies to the system.
- **System Software:** The special software within the cryptographic boundary (e.g., operating system, compilers or utility programs) designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system, and associated programs, and data. [4]
- **Third Party Protection:** The protection of non-involved parties from damage consequential to an attack and any resulting response.
- **Threat:** The potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. [3]
- **Threat Action:** An assault on system security. [3]
- **Threat Analysis:** The analysis of the probability of occurrences and consequences of damaging actions to a system. [3]
- **Threat Consequence:** A security violation that results from a threat action. [3]
- **Throughput:** The rate that a device can successfully deliver messages without dropping a single packet. [2]
- **Traffic Analysis:** Inference of information from observable characteristics of data flow(s), even when the data is encrypted or otherwise not directly available, including the identities and locations of source(s) and destination(s), and the presence, amount, frequency, and duration of occurrence.
- **Trojan Horse:** A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program. [3]
- **Unauthorized access:** Unauthorized access encompasses a range of incidents from improperly logging into a user's account (e.g., when a hacker logs in to a legitimate user's account) to obtaining unauthorized access to files and directories possibly by obtaining "super-user" privileges. Unauthorized access also includes access to network data gained by planting an unauthorized "sniffer" program to capture all packets traversing the network at a particular point.
- **User:** A person, organization entity, or automated process that accesses a system, whether authorized to do so or not. [3]
- **Virtual Private Network (VPN):** A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network.
- **Virus**: Self replicating, malicious program segment that attaches itself to an application program or other executable system component and leaves no external signs of its presence.

- **Vulnerability:** A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's integrity or security policy. [3]
- **Wide Area Network (WAN):** A communications network designed to connect computers over a large distance, such as across the country or world. [4]
- **Wiretapping:** An attack that intercepts and accesses data and other information contained in a flow in a communication system. [3]

  NOTE 1: Although the term originally referred to making a mechanical connection to an electrical conductor that links two nodes, it is now used to refer to reading information from any sort of medium used for a link or even directly from a node, such as gateway or sub-network switch.

  NOTE 2: "Active wiretapping" attempts to alter the data or otherwise affect the flow; "passive wiretapping" only attempts to observe the flow and gain knowledge of information it contains.
- **Worm:** A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively. [3]
- **Zone:** A set of network segments, network devices, and hosts for which the same security policies and requirements are valid.

  NOTE: A zone has a clear border with other zones. The security policy of a zone is typically enforced by a combination of mechanisms both at the zone edge and within the zone. Zones can be hierarchical.

Appendix E – References Documents

American National Standards Institute (ANSI)/International Society of Automation (ISA)-95.00.01-2000, *Enterprise-Control System Integration Part 1: Models and Terminology*

ANSI/ISA0-99.00.01-2007, *Security for Industrial Automation and Control Systems: Terminology, Concepts, and Models*

ANSI/ISA-99.02.01-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*

Interstate Natural Gas Association of America (INGAA) *Interstate Natural Gas Pipeline Efficiency*

National Institute of Standards and Technology (NIST) SP 800-16 Rev 1, Draft *Information Security Training Requirements: A Role- and Performance-Based Model*

NIST SP 800-36, *Guide to Selecting Information Technology Security Products*

NIST SP 800-48, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*

NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*

NIST SP 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*

NIST SP 800-53 Rev 3, *Recommended Security Controls for Federal Information Systems and Organizations*

NIST SP 800-53A Rev 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*

NIST SP 800-61 Rev 1, *Computer Security Incident Handling Guide*

NIST SP 800-63, *Electronic Authentication Guideline*

NIST SP 800-73, *Interfaces for Personal Identity Verification*

NIST SP 800-76, *Biometric Data Specification for Personal Identity Verification*

NIST SP 800-82, *Final Public Draft, Guide to Industrial Control Systems (ICS) Security*

NIST SP 800-83, *Guide to Malware Incident Prevention and Handling*

NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*

NIST SP800-97 *Establishing Robust Security Networks:* Draft, *Guide to IEEE 802.11i*

U.S. Department of Energy, *21 Steps to Improve Cyber Security of SCADA Networks*

U.S Department of Homeland Security, *National Infrastructure Protection Plan*

U.S Department of Homeland Security, National Cyber Security Division, *Catalog of Control Systems Security: Recommendations for Standards Developers*

U.S. General Accounting Office (GAO)-04-321, *Technology Assessment: Cybersecurity for Critical Infrastructure Protection*

U.S. GAO-04-354, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*

APPENDIX F

Guidance for Implementing National Institute of Standards and Technology's (NIST)

Framework for Improving Critical Infrastructure Cybersecurity

Introduction

In collaboration with a large number of public and private sector groups, INGAA participated in the development of National Institute of Standards and Technology's ("NIST") *Framework for Improving Critical Infrastructure Cybersecurity (Framework)*, which was initiated in response to President Obama's 2013 Executive Order 13636: Improving Critical Infrastructure Cybersecurity. The *Framework* was issued in February 2014 and incorporates a risk management structure that includes elements of a maturity model, and recommends information sharing. The *Framework* is intended for all organizations with critical systems. It is technology and industry neutral and intended to complement, not replace, an organization's risk management process and cybersecurity program by providing tools to help an organization identify gaps in its practices and develop a roadmap for continuous improvement.

Since the issuance of the *Framework*, INGAA members have devoted significant resources to the development and planned implementation of the *Framework's* standards for control systems, INGAA member companies' most critical assets. Member companies found that the NIST *Framework* is consistent with the path taken in INGAA's *Control Systems Cyber Security Guidelines*. Rather than rewrite its guidelines using suggested alternative models, INGAA has added this guide as an appendix to include components from the *Framework*.

The guide is intended as a tool, and not intended to impose any obligations upon the owner/operator of a natural gas pipeline. As contemplated by NIST, the decision to adopt the voluntary *Framework* will be based upon each company's individual assessment of its security requirements, risk tolerances and resources.

USING THE GUIDE

The NIST *Framework* is comprised of three primary components: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. The Framework Core addresses five basic Functions to be included in an organization's cybersecurity risk management program: Identify, Protect, Detect, Respond, and Recover.

The appendix is broken down into five sections to represent each of the *Framework's* Core Functions. Each section is then broken down by category within those functions. Each section also includes Additional Requirements that may be triggered by voluntary adoption of the *Framework*, and examples of Implementing Policies, Procedures and Actions that a company may consider to enhance its cybersecurity posture.

Identify

NIST Framework for Improving Critical Infrastructure Cybersecurity

Identify: Asset Management (ID.AM)

The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

ID.AM-1: Inventory physical devices and systems.

ID.AM-2: Inventory software platforms and applications.

ID.AM-3: Map organization communication and data flows.

ID.AM-4: External information systems are catalogued.

ID.AM-5: Prioritize resources (e.g., hardware, devices, data, and software) based on classification, criticality, and business value.

ID.AM-6: Establish cybersecurity roles and responsibilities for workforce and third-party stakeholders (e.g., suppliers, customers, and partners).

Additional Guidelines

Operators should develop procedures, using consistent criteria, for identifying criticality and maintaining inventory of:

1. critical physical devices (ID.AM-1);
2. critical software assets (ID.AM-2);
3. critical asset data flows (and maintain a map of critical data flows) (ID.AM-3); and
4. critical external systems (ID.AM-4).

Operators should develop procedures to prioritize resources based on classification, criticality, and business value. (ID.AM-5)

Operators should maintain a governance system that establishes an individual or organization that has defined roles and responsibilities for managing cybersecurity risk and maintain third party management process that defines their roles and responsibilities in managing cybersecurity risk. (ID.AM-6)

Examples of Implementing Policies, Procedures and Actions

1. Incident Response Plan
2. Corporate Cyber Security Policy
3. Asset Management Policy
4. Software License Policy

5. Incident Management Procedures
6. IT Inventory Procedure
7. Information Distribution Procedure

NIST Framework for Improving Critical Infrastructure Cybersecurity

Identify: Business Environment (ID.BE)

The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

ID.BE-1: Identify and communicate organization's role in the supply chain.

ID.BE-2: Identify and communicate the organization's place in critical infrastructure and its industry sector.

ID.BE-3: Establish and communicate priorities for organizational mission, objectives, and activities.

ID.BE-4: Establish dependencies and critical functions for delivery of critical services.

ID.BE-5: Establish resilience requirements to support delivery of critical services.

Additional Guidelines

Operators should refer to TSA Requirements criticality screening process. (ID.BE-1)

Operators should participate, where applicable, in the TSA top 100 critical systems. (ID.BE-2)

Operators should develop procedures for establishing priorities. (ID.BE-3)

- Procedures should use consistent criteria to determine cyber resource criticality.
- Operators should maintain the prioritization within the critical cyber resources.
- Operators should utilize the organizational mission, objectives, and activities to inform cybersecurity roles, responsibilities, and risk management decisions.

Operators should develop procedures to establish dependencies and critical functions for the delivery of critical services. (ID.BE-4)

Operators should establish resilience requirements to support delivery of critical assets. (ID.BE-5).

Examples of Implementing Policies, Procedures and Actions

1. Incident Response Plan
2. Corporate Cyber Security Policy
3. Business Continuity Standards
4. Disaster Recovery Plan

NIST Framework for Improving Critical Infrastructure Cybersecurity

Identify: Risk Assessment (ID.RA)

The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

ID.RA-1: Identify and document asset vulnerabilities.

ID.RA-2: Receive threat and vulnerability information from information sharing forums and sources.

ID.RA-3: Identify and document threats.

ID.RA-4: Identify potential business impacts and likelihoods.

ID.RA-5: Use threats, vulnerabilities, likelihoods, and impacts to determine risk.

ID.RA-6: Identify and prioritize risk responses.

Additional Guidelines

Operators may consider establishing procedures to receive and analyze threat and vulnerability information is from information sharing forums and sources on an ongoing basis. (ID.RA-2)

Operators should develop strategies to identify both internal and external threats on an ongoing basis, as well as procedures for documenting those threats. (ID.RA-3)

Operators should develop processes to identify potential business impacts and likelihoods of documented threats. (ID.RA-4)

Operators should develop processes to use identified threats, vulnerabilities, likelihoods, and impacts to minimize risk. (ID.RA-5)

Operators should implement strategies to identify and prioritize risk responses. (ID.RA-6)

Examples of Implementing Policies, Procedures and Actions

1. Network Intrusion Detection Procedure
2. Network Device Access Procedure
3. Elevated Privileges Procedure
4. Risk and Vulnerability Assessment

NIST Framework for Improving Critical Infrastructure Cybersecurity

Identify: Risk Management Strategy (ID.RM)

The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

ID.RM-1: Establish, manage and agree to risk management processes.

ID.RM-2: Determine and clearly express organizational risk tolerance.

ID.RM-3: Critical infrastructure role will inform risk tolerance determination.

Additional Guidelines

Operators should establish risk management processes, with agreement from organizational stakeholders. (ID.RM-1)

Operators may consider developing processes to determine and clearly express organizational risk tolerance. (ID.RM-2)

Operators should be informed by their role in critical infrastructure and sector specific risk analysis in determining its risk tolerance. (ID.RM-3)

Examples of Implementing Policies, Procedures and Actions

1. Incident Response Plan
2. Corporate Cyber Security Policy
3. Business Continuity Standards
4. Cyber Event Restoral Procedures
5. Disaster Recovery Plan

NIST Framework for Improving Critical Infrastructure Cybersecurity

Identify: Governance (ID.GV)

The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

ID.GV-1: Establish organizational information security policy.

ID.GV-2: Coordinate and align information security roles & responsibilities with internal roles and external partners.

ID.GV-3: Understand and manage legal and regulatory requirements, including privacy and civil liberties obligations.

ID.GV-4: Address cybersecurity risks in governance and risk management processes.

Additional Guidelines

Operators should establish an organizational information security policy. (ID.GV-1)

Operators should develop procedures to identify and manage legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations. (ID.GV-3)

Operators should develop a strategy to establish organizational governance and risk management processes to address cybersecurity risks. (ID.GV-4)

Examples of Implementing Policies, Procedures and Actions

1. Corporate Cyber Security Policy
2. SOX
3. Security Roles and Responsibilities

Protect

NIST Framework for Improving Critical Infrastructure Cybersecurity

Protect: Access Control (PR.AC)

Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.

PR.AC-1: Manage identities and credentials for authorized devices and users.

PR.AC-2: Manage and protect physical access to assets.

PR.AC-3: Manage remote access.

PR.AC-4: Manage access permissions, incorporating the principles of least privilege and separation of duties.

PR.AC-5: Protect network integrity, incorporating network segregation where appropriate.

Additional Guidelines

Operators must incorporate the concept of least privilege and separation of duties in managing access to critical systems. (PR.AC-4)

Examples of Implementing Policies, Procedures and Actions

Electronic Communication Policy

Electronic Information Security Policy

Remote Access to Internal Network Connection Standard

IT Segregation of Duties Standard

Electronic Communication Standard

Change Control Standard

NIST Framework for Improving Critical Infrastructure Cybersecurity

Protect: Awareness and Training (PR.AT)

The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.

PR.AT-1: Inform and train all users.

PR.AT-2: Privileged users understand roles & responsibilities.

PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, and partners) understand roles & responsibilities.

PR.AT-4: Senior executives understand roles & responsibilities.

PR.AT-5: Physical and information security personnel understand roles & responsibilities.

Additional Guidelines

Operators may consider implementing differentiated security-specific training tailored to specific roles & responsibilities for each:

- privileged users
- party stakeholders
- senior executives,
- Physical and information security personnel. (PR.AT-2, PR.AT-3, PR.AT-4, PR.AT-5)

Examples of Implementing Policies, Procedures and Actions

1. Personnel Security Communication and Training Procedure

NIST Framework for Improving Critical Infrastructure Cybersecurity

Protect: Data Security (PR.DS)

Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

PR.DS-1: Protect data-at-rest.

PR.DS-2: Protect data-in-transit.

PR.DS-3: Formally manage assets throughout removal, transfers, and disposition.

PR.DS-4: Maintain adequate capacity to ensure availability.

PR.DS-5: Implement protections against data leaks.

PR.DS-6: Use integrity checking mechanisms to verify software, firmware, and information integrity.

PR.DS-7: Separate the development and testing environment(s) from the production environment.

Additional Guidelines

Operators may consider developing protection processes for data-at-rest for control systems and other critical systems. (PR.DS-1)

Operators may consider developing protection processes for data-in-transit for control systems and other critical systems. (PR.DS-2)

Operators may consider developing formal procedures to manage the transfer and disposition of assets in critical control systems. (PR.DS-3)

Operators should develop procedures to maintain adequate system storage capacity to ensure the full performance and availability of critical control systems and associated monitoring activities. (PR.DS-4)

- Regular audit of storage capacity.
- Develop procedures for the transfer of records from critical control system devices to a separate system or other storage media.

Operators may consider developing processes to protect the validity of control system firmware and information integrity on control system devices. (PR.DS-6)

- Employ verification tools to, for example, verify current system integrity, detect unauthorized changes to firmware and systems information, and detect potential integrity violations.
- Generate audit reports for analysis.

Operators should separate control systems development and/or testing environment(s) (where applicable) from the production environment. (PR.DS-7)

Examples of Implementing Policies, Procedures and Actions

1. Asset Management Policy
2. Information Distribution Procedure

NIST Framework for Improving Critical Infrastructure Cybersecurity

Protect: Information Protection Processes and Procedures (PR.IP)

Security policies (that address purpose, scope, roles, responsibilities, management, commitment, and coordination among organizational entities), processes and procedures are maintained and used to manage protection of information systems and assets.

PR.IP-1: Create and maintain a baseline configuration of information technology/industrial control systems.

PR.IP-2: Implement a System Development Life Cycle to manage systems.

PR.IP-3: Put in place configuration change control processes.

PR.IP-4: Conduct, maintain, and periodically test information backups.

PR.IP-5: Ensure meeting the policy and regulations regarding the physical operating environment for organizational assets.

PR.IP-6: Destroy data according to policy.

PR.IP-7: Continuously improve the protection processes.

PR.IP-8: Share the effectiveness of protection technologies with the appropriate parties.

PR.IP-9: Put in place and manage response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery).

PR.IP-10: Test the response and recovery plans.

PR.IP-11: Include cybersecurity in the human resources practices (e.g., deprovisioning, personnel screening).

PR.IP-12: Develop and implement a vulnerability management plan.

Additional Guidelines

Operators should establish and maintain a baseline configuration of critical control systems. (PR.IP-1)

- Baseline configurations should be documented, formally reviewed, and agreed-upon sets of specifications and configurations of those systems.
- Employ mechanisms (e.g., automated system tools) to maintain up-to-date, complete, accurate, and readily available information.
- Establish periodic review and approval process for updates to the baseline configuration.

Operators may consider developing policy and procedures for control system data handling and data destruction to ensure that information receives appropriate protection to avoid unauthorized disclosure. (PR.IP-6)

Operators should develop processes for the continuous monitoring of protection processes for critical systems, to identify areas for Improvement and implement necessary process Improvements. (PR.IP-7)

Operators may consider developing strategies to facilitate sharing information on effectiveness of protection strategies with key stakeholders. (PR.IP-8)

Operators should develop cybersecurity procedures to be incorporated into human resources functions (e.g., background checks/personnel screening in accordance with relevant laws, deprovisioning and return of company assets upon separation, etc.). (PR.IP-11)

Examples of Implementing Policies, Procedures and Actions

1. Electronic Communication Policy
2. Electronic Information Security Policy
3. Change Management Procedure
4. Personnel Management Procedure
5. Application Software Restrictions
6. Network Equipment Build Requirements

NIST Framework for Improving Critical Infrastructure Cybersecurity

Protect: Maintenance (PR.MA)

Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.

PR.MA-1: Perform maintenance and repair of organizational assets and log in a timely manner, with approved and controlled tools.

PR.MA-2: Approve, log, and performance remote maintenance of organizational assets in a manner that prevents unauthorized users.

Additional Guidelines

Operators should develop processes to perform and log maintenance and repair activities for critical system assets in a timely manner, with approved and controlled tools. (PR.MA-1)

Operators should develop processes to approve, log, and, perform remote maintenance of organizational assets in a manner that prevents unauthorized access. (PR.MA-2)

Examples of Implementing Policies, Procedures and Actions

1. Change Management Policy
2. IT Segregation of Duties Standard
3. Network Device Access Procedure
4. Personnel Management Procedure

NIST Framework for Improving Critical Infrastructure Cybersecurity

Protect: Protective Technology (PR.PT)

Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

PR.PT-1: Determine, document, implement, and review audit/log records in accordance with the policy set in place.

PR.PT-2: Protect removable media and restrict its use according to the policy.

PR.PT-3: Control, by incorporating the principle of least functionality, the access to systems and assets.

PR.PT-4: Protect communications and control networks.

Additional Guidelines

Operators should determine, document, and review audit/log records in accordance with the security policy in place. (PR.PT-1)

Operators should develop processes to control access to all critical systems and assets by incorporating the principle of least functionality. (PR.PT-3)

Operators must implement procedures to protect all critical communications and control networks. (PR.PT-4)

Examples of Implementing Policies, Procedures and Actions

1. Electronic Communication Policy
2. Integrated Security Plan

Detect

NIST Framework for Improving Critical Infrastructure Cybersecurity

Detect: Anomalies and Events (DE.AE)

Anomalous activity is detected in a timely manner and the potential impact of events is understood.

DE.AE-1: Establish and manage a baseline of network operations and expected data flows for uses and systems.

DE.AE-2: Analyze detected events to understand attack targets and methods.

DE.AE-3: Aggregate and correlate event data from multiple sources and sensors.

DE.AE-4: Determine the impact of events.

DE.AE-5: Establish incident alert thresholds.

Additional Guidelines

Operators should establish and manage a baseline of network operations and expected data flows for uses and systems. (DE.AE-1)

- Operators should establish a baseline of normal network operations of critical systems.
- Operators may consider establishing a baseline of normal network operations with externally connected systems.
- Operators should establish a baseline of normal data flows for critical systems.
- Operators may consider establishing a baseline of normal data flows with externally connected systems.
- These baselines should be included in a configuration control document for the associated information system.

Operators should analyze detected events for indicators of unusual or inappropriate activity. (DE.AE-2)

- Operators may consider using the following to gain insight into a detected event: (i) ISAC, (ii) ICS-CERT / US-CERT, (iii) SANS, and (iv) Internal support staff

Operators may consider collecting and aggregating data from multiple information system sources for analysis on indicators, targets, and methods for attack. (DE.AE-3)

Operators should analyze the impact of events consistent with their established response plan(s) for critical systems. (DE.AE-4)

Operators should define incidence types and severities and the levels which trigger additional action(s) for critical systems. (DE.AE-5)

Examples of Implementing Policies, Procedures and Actions

1. Integrated Security Plan
2. Network Intrusion Detection Procedure

NIST Framework for Improving Critical Infrastructure Cybersecurity

Detect: Security Continuous Monitoring (DE.CM)

The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.

DE.CM-1: Monitor network to detect potential cybersecurity events.

DE.CM-2: Monitor the physical environment to detect potential cybersecurity events.

DE.CM-3: Monitor personnel activity to detect potential cybersecurity events.

DE.CM-4: Detect malicious code.

DE.CM-5: Detect unauthorized mobile code.

DE.CM-6: Monitor external service provider activity to detect potential cybersecurity events.

DE.CM-7: Perform monitoring for unauthorized personnel, connections, devices, and cybersecurity events

DE.CM-8: Perform vulnerability scans.

Examples of Implementing Policies, Procedures and Actions

1. Integrated Security Plan
2. Network Intrusion Detection Procedure
3. System Risk and Vulnerability Assessment
4. Virus Protection Procedure
5. Malware Protection Procedure
6. Security Audit Logging Procedure
7. User Account Controls and Monitoring

NIST Framework for Improving Critical Infrastructure Cybersecurity

Detect: Detections Processes (DE.DP)

Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability.

DE.DP-2: Ensure that detection activities comply with all applicable Requirements.

DE.DP-3: Test detection processes.

DE.DP-4: Communicate event detection information to appropriate parties.

DE.DP-5: Continuously improve detection processes.

Additional Guidelines

Operators should develop processes to ensure that detection activities for critical systems comply with all applicable legal and contractual Requirements. (DE.DP-2)

Operators should implement procedures for regular testing of detection processes for all critical systems. (DE.DP-3)

Operators should develop processes to communicate event detection information to responsible personnel and other key internal stakeholders and appropriate members of the executive and management teams. (DE.DP-4)

- Identify personnel who will support the incident and act in key decision-making roles.
- Devise standards for assembly of necessary information for (i) periodic informational communications, and (ii) timely communication following an event.

Operators may consider developing formalized processes to continuously improve detection processes. (DE.DP-5)

- Capture and collect current analysis and lessons learned from key personnel following detection(s) and/or testing.
- Schedule periodic updates to detection processes to incorporate updated analysis and lessons learned.
- Develop accelerated update process for critical vulnerabilities.

Examples of Implementing Policies, Procedures and Actions

1. Integrated Security Plan
2. Network Intrusion Detection Procedure
3. System Risk and Vulnerability Assessment
4. Security Testing Protocols

RESPOND

NIST Framework for Improving Critical Infrastructure Cybersecurity

Respond: Response Planning (RS.RP)

Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.

RS.RP-1: Execute response plan during or after an event.

Additional Guidelines

Operators must promptly execute critical systems response plan(s) during or immediately after an event. (RS.RP-1)

Examples of Implementing Policies, Procedures and Actions

1. Incident Recourse Plan
2. Business Continuity Standards
3. Cyber Event Restoral Procedure
4. Incident Management Procedure
5. Disaster Recovery Plan

NIST Framework for Improving Critical Infrastructure Cybersecurity

Respond: Communications (RS.CO)

Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.

RS.CO-1: When a response is needed, personnel know their roles and order of operations.

RS.CO-2: Report events consistent with established criteria.

RS.CO-3: Share information consistent with response plans.

RS.CO-4: Coordination with stakeholders is consistent with response plans.

RS.CO-5: Information is voluntarily shared with stakeholders to achieve broader cybersecurity situational awareness.

Additional Guidelines

Operators should consider developing reporting protocols and/or communications procedures consistent with roles and responsibilities defined in event response plan(s). (RS.CO-1, RS.CO-2)

- Identify management and other personnel who will support the incident and act in key decision-making roles.
- Document reporting structure based on roles and decision-making authorities.
- Devise guidelines for timing, method(s) of communication, and information to be communicated among key personnel during response.

Operators may consider developing procedures in coordination with response plan to communicate and facilitate information sharing among key internal stakeholders and executive and management teams during response. (RS.CO-3, RS.CO-4)

- Identify management and other personnel who will support the incident and act in key decision-making roles.
- Devise framework for timing, methods of communication, and assembly of information to be communicated to key personnel during response.

Operators may consider developing guidelines for sharing response information with all personnel, including employees and contractors, regarding response(s) to events impacting critical or control systems. (RS.CO-5)

- Share information to achieve broader cybersecurity situational awareness.
- Publish information regarding reporting computer anomalies and incidents to the incident handling team.

Such information may be included in routine employee awareness activities.

Examples of Implementing Policies, Procedures and Actions

1. Incident Response Plan
2. Business Continuity Standards
3. Cyber Event Restoral Procedure
4. Incident Management Procedure
5. Disaster Recovery Plan

NIST Framework for Improving Critical Infrastructure Cybersecurity

Respond: Analysis (RS.AN)

Analysis is conducted to ensure adequate response and support recovery activities.

RS.AN-1: Investigate notifications from detection systems.

RS.AN-2: Understand the impact of the incident.

RS.AN-3: Perform forensics.

RS.AN-4: Categorize incidents consistent with response plans.

Additional Guidelines

Operators should implement procedures for investigating notifications from detection systems for all critical systems. (RS.AN-1)

Operators should analyze the impact of events consistent with their established response plan(s) for critical control systems. (RS.AN-2)

Operators should perform forensic analysis of incidents with potentially material impact on operation of control systems. (RS.AN-3)

- Collect event data including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, network monitoring, physical access monitoring, and user/administrator reports.
- Evaluate details, trends, and handling of events.
- Operators should categorize control system incidents analyzed consistent with response plan(s) for analysis to ensure a consistent and effective approach to the management of information security. (RS.AN-4)

Examples of Implementing Policies, Procedures and Actions

1. Business Continuity Standards
2. Cyber Event Restoral Procedure
3. Incident Management Procedure
4. Disaster Recovery Plan

NIST Framework for Improving Critical Infrastructure Cybersecurity

Respond: Mitigation (RS.MI)

Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.

RS.MI-1: Contain incidents.

RS.MI-2: Mitigate incidents.

RS.MI-3: Mitigate or document newly identified vulnerabilities as accepted risks.

Additional Guidelines

Operators should develop processes to ensure a consistent, effective approach to contain incidents impacting critical systems. (RS.MI-1)

Operators should develop processes to ensure a consistent, effective approach to mitigating any effects of incidents impacting critical systems. (RS.MI-2)

Operators may consider developing a process to risk-rate newly identified control system vulnerabilities to determine whether mitigation is necessary. (RS.MI-3)

Examples of Implementing Policies, Procedures and Actions

1. Incident Response Plan
2. Business Continuity Standards
3. Cyber Event Restoral Procedure
4. Incident Management Procedure
5. Disaster Recovery Plan

NIST Framework for Improving Critical Infrastructure Cybersecurity

Respond: Improvements (RS.IM)

Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

RS.IM-1: Incorporate lessons learned in response plans.

RS.IM-2: Update response strategies.

Additional Guidelines

Operators may consider developing formalized processes to continuously improve response activities. (RS.IM-1, RS.IM-2)

- Capture and collect event details and lessons learned from key personnel following response.
- Schedule periodic updates to response processes and incorporate lessons learned.
- Develop accelerated update process for critical vulnerabilities.

Examples of Implementing Policies, Procedures and Actions

1. Business Continuity Standards
2. Cyber Event Restoral Procedure
3. Incident Management Procedure
4. Disaster Recovery Plan

RECOVER

NIST Framework for Improving Critical Infrastructure Cybersecurity

Recover: Recovery Planning (RC.RP)

Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.

RC.RP-1: Execute recovery plan during or after an event.

Additional Guidelines

Operators must promptly execute critical systems restoration and recovery plan(s) during or immediately after an event. (RC.RP-1)

Operators should develop procedures for identification of critical physical device(s) necessary to execute critical systems restoration and recovery plan(s). (RC.RP-1)

Examples of Implementing Policies, Procedures and Actions

1. Incident Response Plan
2. Business Continuity Standards
3. Cyber Event Restoral Procedure
4. Disaster Recovery Plan

NIST Framework for Improving Critical Infrastructure Cybersecurity

Recover: Improvements (RC.IM)

Recovery planning and processes are improved by incorporating lessons learned into future activities.

RC.IM-1: Incorporate lessons learned into recovery plans.

RC.IM-2: Update recovery strategies.

Additional Guidelines

Operators should develop formalized processes to capture and collect lessons learned from key personnel following the response to an event. (RC.IM-1)

Operators should develop procedures to update critical systems recovery strategies in response to lessons learned. (RC.IM-2)

Examples of Implementing Policies, Procedures and Actions

1. Business Continuity Standards
2. Cyber Event Restoral Procedure
3. Disaster Recovery Plan

NIST Framework for Improving Critical Infrastructure Cybersecurity

Recover: Communications (RC.CO)

Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.

RC.CO-1: Manage public relations.

RC.CO-2: Repair reputation after an event.

RC.CO-3: Communicate recovery activities to internal stakeholders and executive and management teams.

Additional Guidelines

Operators should incorporate public relations management into critical systems restoration and recovery plan(s). (RC.CO-1)

- Ensure that there are written incident response procedures.
- Define personnel roles and identify management who will support public relations matters following an event.
- Assign roles and duties for managing public relations.
- Devise standards for the time required for response to an event.
- Assemble and maintain third-party contact information to be used to report and/or response to an event.
- Conduct periodic scenario sessions for key personnel to ensure that they understand current threats or risks, and their responsibilities in public relations response.

Operators should take proactive steps following an event to implement public relations plans and mitigate impacts and/or repair reputation. (RC.CO-2)

Operators should develop procedures to communicate recovery activities to key internal stakeholders and executive and management teams. (RC.CO-3)

- Identify management and other personnel who will support the incident and act in key decision-making roles.
- Devise standards for timing and assembly of information to be communicated to key personnel following an event.

Examples of Implementing Policies, Procedures and Actions

1. Incident Response Plan
2. Business Continuity Standards
3. Cyber Event Restoral Procedure
4. Disaster Recovery Plan