Executive Summary

This document provides guidance for establishing secure industrial control systems (ICS). These ICS, which include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as skid-mounted Programmable Logic Controllers (PLC) are often found in the industrial control sectors. ICS are typically used in industries such as electric, water and wastewater, oil and natural gas, transportation, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (e.g., automotive, aerospace, and durable goods.) SCADA systems are generally used to control dispersed assets using centralized data acquisition and supervisory control. DCS are generally used to control production systems within a local area such as a factory using supervisory and regulatory control. PLCs are generally used for discrete control for specific applications and generally provide regulatory control. These control systems are vital to the operation of the U.S. critical infrastructures that are often highly interconnected and mutually dependent systems. It is important to note that approximately 90 percent of the nation's critical infrastructures are privately owned and operated. Federal agencies also operate many of the ICS mentioned above; other examples include air traffic control and materials handling (e.g., Postal Service mail handling.) This document provides an overview of these ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.

Initially, ICS had little resemblance to traditional information technology (IT) systems in that ICS were isolated systems running proprietary control protocols using specialized hardware and software. Widely available, low-cost Internet Protocol (IP) devices are now replacing proprietary solutions, which increases the possibility of cyber security vulnerabilities and incidents. As ICS are adopting IT solutions to promote corporate business systems connectivity and remote access capabilities, and are being designed and implemented using industry standard computers, operating systems (OS) and network protocols, they are starting to resemble IT systems. This integration supports new IT capabilities, but it provides significantly less isolation for ICS from the outside world than predecessor systems, creating a greater need to secure these systems. While security solutions have been designed to deal with these security issues in typical IT systems, special precautions must be taken when introducing these same solutions to ICS environments. In some cases, new security solutions are needed that are tailored to the ICS environment.

Although some characteristics are similar, ICS also have characteristics that differ from traditional information processing systems. Many of these differences stem from the fact that logic executing in ICS has a direct affect on the physical world. Some of these characteristics include significant risk to the health and safety of human lives and serious damage to the environment, as well as serious financial issues such as production losses, negative impact to a nation’s economy, and compromise of proprietary information. ICS have unique performance and reliability requirements and often use operating systems and applications that may be considered unconventional to typical IT personnel. Furthermore, the goals of safety and efficiency sometimes conflict with security in the design and operation of control systems.

Originally, ICS implementations were susceptible primarily to local threats because many of their components were in physically secured areas and the components were not connected to IT networks or systems. However, the trend toward integrating ICS systems with IT networks provides significantly less isolation for ICS from the outside world than predecessor systems, creating a greater need to secure these systems from remote, external threats. Also, the increasing use of wireless networking places ICS implementations at greater risk from adversaries who are in relatively close physical proximity but do not have direct physical access to the equipment. Threats to control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, malicious intruders, complexities, accidents, natural disasters as well as malicious or accidental actions by insiders. ICS security objectives typically follow the priority of availability, integrity and confidentiality, in that order.

Possible incidents an ICS may face include the following:

- Blocked or delayed flow of information through ICS networks, which could disrupt ICS operation
- Unauthorized changes to instructions, commands, or alarm thresholds, which could damage, disable, or shut down equipment, create environmental impacts, and/or endanger human life
- Inaccurate information sent to system operators, either to disguise unauthorized changes, or to cause the operators to initiate inappropriate actions, which could have various negative effects
- ICS software or configuration settings modified, or ICS software infected with malware, which could have various negative effects
- Interference with the operation of safety systems, which could endanger human life.

Major security objectives for an ICS implementation should include the following:

- **Restricting logical access to the ICS network and network activity.** This includes using a demilitarized zone (DMZ) network architecture with firewalls to prevent network traffic from passing directly between the corporate and ICS networks, and having separate authentication mechanisms and credentials for users of the corporate and ICS networks. The ICS should also use a network topology that has multiple layers, with the most critical communications occurring in the most secure and reliable layer.
- **Restricting physical access to the ICS network and devices.** Unauthorized physical access to components could cause serious disruption of the ICS's functionality. A combination of physical access controls should be used, such as locks, card readers, and/or guards.
- **Protecting individual ICS components from exploitation.** This includes deploying security patches in as expeditious a manner as possible, after testing them under field conditions; disabling all unused ports and services; restricting ICS user privileges to only those that are required for each person's role; tracking and monitoring audit trails; and using security controls such as antivirus software and file integrity checking software where technically feasible to prevent, deter, detect, and mitigate malware.
- **Maintaining functionality during adverse conditions.** This involves designing the ICS so that each critical component has a redundant counterpart. Additionally, if a component fails, it should fail in a manner that does not generate unnecessary traffic on the ICS or other networks, or does not cause another problem elsewhere, such as a cascading event.
- **Restoring system after an incident.** Incidents are inevitable and an incident response plan is essential. A major characteristic of a good security program is how quickly a system can be recovered after an incident has occurred.

To properly address security in an ICS, it is essential for a cross-functional cyber security team to share their varied domain knowledge and experience to evaluate and mitigate risk to the ICS. The cyber security team should consist of a member of the organization's IT staff, control engineer, control system operator, network and system security expert, a member of the management staff, and a member of the physical security department at a minimum. For continuity and completeness, the cyber security team should consult with the control system vendor and/or system integrator as well. The cyber security team should report directly to site management (e.g., facility superintendent) or the company's CIO/CSO, who in turn, accepts complete responsibility and accountability for the cyber security of the ICS. An effective cyber security program for an ICS should apply a strategy known as "defense-in-depth", layering security mechanisms such that the impact of a failure in any one mechanism is minimized.

In a typical ICS this means a defense-in-depth strategy that includes:

- Developing security policies, procedures, training and educational material that apply specifically to the ICS.
- Considering ICS security policies and procedures based on the Homeland Security Advisory System Threat Level, deploying increasingly heightened security postures as the Threat Level increases.
- Addressing security throughout the lifecycle of the ICS from architecture design to procurement to installation to maintenance to decommissioning.
- Implementing a network topology for the ICS that has multiple layers, with the most critical communications occurring in the most secure and reliable layer.
- Providing logical separation between the corporate and ICS networks (e.g., stateful inspection firewall(s) between the networks).
- Employing a DMZ network architecture (i.e., prevent direct traffic between the corporate and ICS networks).
- Ensuring that critical components are redundant and are on redundant networks.
- Designing critical systems for graceful degradation (fault tolerant) to prevent catastrophic cascading events.
- Disabling unused ports and services on ICS devices after testing to assure this will not impact ICS operation.
- Restricting physical access to the ICS network and devices.
- Restricting ICS user privileges to only those that are required to perform each person's job (i.e., establishing role-based access control and configuring each role based on the principle of least privilege).
- Considering the use of separate authentication mechanisms and credentials for users of the ICS network and the corporate network (i.e., ICS network accounts do not use corporate network user accounts).
- Using modern technology, such as smart cards for Personal Identity Verification (PIV).
- Implementing security controls such as intrusion detection software, antivirus software and file integrity checking software, where technically feasible, to prevent, deter, detect, and mitigate the introduction, exposure, and propagation of malicious software to, within, and from the ICS.
- Applying security techniques such as encryption and/or cryptographic hashes to ICS data storage and communications where determined appropriate.
- Expeditiously deploying security patches after testing all patches under field conditions on a test system if possible, before installation on the ICS.
- Tracking and monitoring audit trails on critical areas of the ICS.

2. Overview of Industrial Control Systems

Industrial control system (ICS) is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as skid-mounted Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures. ICS are typically used in industries such as electrical, water and wastewater, oil and natural gas, chemical, transportation, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (e.g., automotive, aerospace, and durable goods.) These control systems are critical to the operation of the U.S. critical infrastructures that are often highly interconnected and mutually dependent systems. It is important to note that approximately 90 percent of the nation's critical infrastructures are privately owned and operated. Federal agencies also operate many of the industrial processes mentioned above; other examples include air traffic control and materials handling (e.g., Postal Service mail handling.) This section provides an overview of SCADA, DCS, and PLC systems, including typical architectures and components. Several diagrams are presented to depict the network connections and components typically found on each system to facilitate the understanding of these systems. Keep in mind that actual implementations of ICS may be hybrids that blur the line between DCS and SCADA systems by incorporating attributes of both. Please note that the diagrams in this section do not represent a secure ICS. Architecture security and security controls are discussed in Section 5 and Section 6 of this document respectively.

2.1 Overview of SCADA, DCS, and PLCs

SCADA systems are highly distributed systems used to control geographically dispersed assets, often scattered over thousands of square kilometers, where centralized data acquisition and control are critical to system operation. They are used in distribution systems such as water distribution and wastewater collection systems, oil and natural gas pipelines, electrical power grids, and railway transportation systems. A SCADA control center performs centralized monitoring and control for field sites over long-distance communications networks, including monitoring alarms and processing status data. Based on information received from remote stations, automated or operator-driven supervisory commands can be pushed to remote station control devices, which are often referred to as field devices. Field devices control local operations such as opening and closing valves and breakers, collecting data from sensor systems, and monitoring the local environment for alarm conditions.

DCS are used to control industrial processes such as electric power generation, oil refineries, water and wastewater treatment, and chemical, food, and automotive production. DCS are integrated as a control architecture containing a supervisory level of control overseeing multiple, integrated sub-systems that are responsible for controlling the details of a localized process. Product and process control are usually achieved by deploying feed back or feed forward control loops whereby key product and/or process conditions are automatically maintained around a desired set point. To accomplish the desired product and/or process tolerance around a specified set point, specific PLCs are employed in the field and proportional, integral, and/or derivative settings on the PLC are tuned to provide the desired tolerance as well as the rate of self-correction during process upsets. DCS are used extensively in process-based industries.

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

The process-based manufacturing industries typically utilize two main processes [1]:

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

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

Both process-based and discrete-based industries utilize the same types of control systems, sensors, and networks. Some facilities are a hybrid of discrete and process-based manufacturing.

While control systems used in distribution and manufacturing industries are very similar in operation, they are different in some aspects. One of the primary differences is that DCS or PLC-controlled sub-systems are usually located within a more confined factory or plant-centric area, when compared to geographically dispersed SCADA field sites. DCS and PLC communications are usually performed using local area network (LAN) technologies that are typically more reliable and high speed compared to the long-distance communication systems used by SCADA systems. In fact, SCADA systems are specifically designed to handle long-distance communication challenges such as delays and data loss posed by the various communication media used. DCS and PLC systems usually employ greater degrees of closed loop control than SCADA systems because the control of industrial processes is typically more complicated than the supervisory control of distribution processes. These differences can be considered subtle for the scope of this document, which focuses on the integration of IT security into these systems. Throughout the remainder of this document, SCADA systems, DCS and PLC systems will be referred to as ICS unless a specific reference is made to one (e.g., field device used in a SCADA system).

2.2 ICS Operation

The basic operation of an ICS is shown in Figure 2-1 [2]. Key components include the following:

- **Control Loop.** A control loop consists of sensors for measurement, controller hardware such as PLCs, actuators such as control valves, breakers, switches and motors, and the communication of variables. Controlled variables are transmitted to the controller from the sensors. The controller interprets the signals and generates corresponding manipulated variables, based on set points, which it transmits to the actuators. Process changes from disturbances result in new sensor signals, identifying the state of the process, to again be transmitted to the controller.
- **Human-Machine Interface (HMI).** Operators and engineers use HMIs to monitor and configure set points, control algorithms, and adjust and establish parameters in the controller. The HMI also displays process status information and historical information.
- **Remote Diagnostics and Maintenance Utilities.** Diagnostics and maintenance utilities are used to prevent, identify and recover from abnormal operation or failures.

A typical ICS contains a proliferation of control loops, HMIs, and remote diagnostics and maintenance tools built using an array of network protocols on layered network architectures. Sometimes these control loops are nested and/or cascading –whereby the set point for one loop is based on the process variable determined by another loop. Supervisory-level loops and lower-level loops operate continuously over the duration of a process with cycle times ranging on the order of milliseconds to minutes.

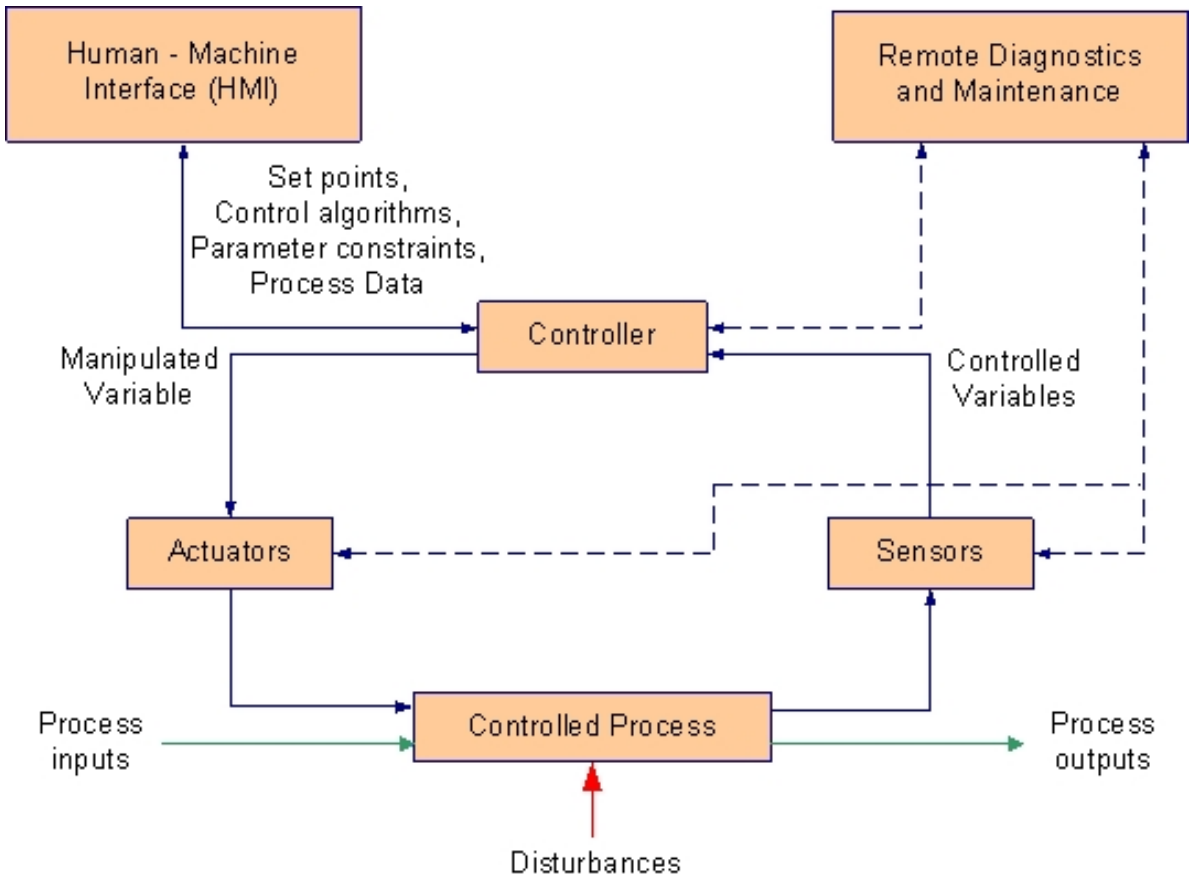

Figure 2-1. ICS Operation

2.3 Key ICS Components

To support subsequent discussions, this section defines key ICS components that are used in control and networking. Some of these components can be described generically for use in SCADA systems, DCS and PLCs, while others are unique to one. The Glossary of Terms in Appendix B contains a more detailed listing of control and networking components. Additionally, Figure 2-5 and Figure 2-6 in Section 2.4 show SCADA implementation examples, Figure 2-7 in Section 2.5 shows a DCS implementation example and Figure 2-8 in Section 2.6 shows a PLC system implementation example that incorporates these components.

2.3.1 Control Components

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

- **Control Server.** The control server hosts the DCS or PLC supervisory control software that communicates with lower-level control devices. The control server accesses subordinate control modules over an ICS network.

- **SCADA Server or Master Terminal Unit (MTU).** 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.

- **Remote Terminal Unit (RTU).** The RTU, also called a remote telemetry unit, is a 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. Sometimes PLCs are implemented as field devices to serve as RTUs; in this case, the PLC is often referred to as an RTU.

- **Programmable Logic Controller (PLC).** The PLC is a small industrial computer originally designed to perform the logic functions executed by electrical hardware (relays, switches, and mechanical timer/counters). PLCs have evolved into controllers with the capability of controlling complex processes, and they are used substantially in SCADA systems and DCS. Other controllers used at the field level are process controllers and RTUs; they provide the same control as PLCs but are designed for specific control applications. In SCADA environments, PLCs are often used as field devices because they are more economical, versatile, flexible, and configurable than special-purpose RTUs.

- **Intelligent Electronic Devices (IED).** An IED is a "smart" sensor/actuator containing the intelligence required to acquire data, communicate to other devices, and perform local processing and control. An IED could combine an analog input sensor, analog output, low-level control capabilities, a communication system, and program memory in one device. The use of IEDs in SCADA and DCS systems allows for automatic control at the local level.

- **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 HMI also allows a control engineer or operator to configure set points or control algorithms and parameters in the controller. The HMI also displays process status information, historical information, reports, and other information to operators, administrators, managers, business partners, and other authorized users. The location, platform, and interface may vary a great deal. 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.

- **Data 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.** The IO server is a control component responsible for collecting, buffering and providing access to process information from control sub-components such as PLCs, RTUs and IEDs. An IO server can reside on the control server or on a separate computer platform. IO servers are also used for interfacing third-party control components, such as an HMI and a control server.

2.3.2 Network 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 control 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:

- **Fieldbus Network.** The fieldbus network links sensors and other devices to a PLC or other controller. Use of fieldbus technologies eliminates the need for point-to-point wiring between the controller and each device. The devices communicate with the fieldbus controller using a variety of protocols. The messages sent between the sensors and the controller uniquely identify each of the sensors.
- **Control Network.** The control network connects the supervisory control level to lower-level control modules.
- **Communications Routers.** A router is a communications device that transfers messages between two networks. Common uses for routers include connecting a LAN to a WAN, and connecting MTUs and RTUs to a long-distance network medium for SCADA communication.
- **Firewall.** 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. Modems are often used in SCADA systems to enable long-distance serial communications between MTUs and remote field devices. They are also used in SCADA systems, DCS and PLCs for gaining remote access for operational and maintenance functions such as entering commands or modifying parameters, and diagnostic purposes.
- **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 remotely access an ICS system.

2.4 SCADA Systems

SCADA systems are used to control dispersed assets where centralized data acquisition is as important as control [3] [4]. These systems are used in distribution systems such as water distribution and wastewater collection systems, oil and natural gas pipelines, electrical utility transmission and distribution systems, and rail and other public transportation systems. SCADA systems integrate data acquisition systems with data transmission systems and HMI software to provide a centralized monitoring and control system for numerous process inputs and outputs. SCADA systems are designed to collect field information, transfer it to a central computer facility, and display the information to the operator graphically or textually, thereby allowing the operator to monitor or control an entire system from a central location in real time. Based on the sophistication and setup of the individual system, control of any individual system, operation, or task can be automatic, or it can be performed by operator commands.

SCADA systems consist of both hardware and software. Typical hardware includes an MTU placed at a control center, communications equipment (e.g., radio, telephone line, cable, or satellite), and one or more geographically distributed field sites consisting of either an RTU or a PLC, which controls actuators and/or monitors sensors. The MTU stores and processes the information from RTU inputs and outputs, while the RTU or PLC controls the local process. The communications hardware allows the transfer of information and data back and forth between the MTU and the RTUs or PLCs. The software is programmed to tell the system what and when to monitor, what parameter ranges are acceptable, and what response to initiate when parameters change outside acceptable values. An IED, such as a protective relay, may communicate directly to the SCADA Server, or a local RTU may poll the IEDs to collect the data and pass it to the SCADA Server. IEDs provide a direct interface to control and monitor equipment and sensors. IEDs may be directly polled and controlled by the SCADA Server and in most cases have local programming that allows for the IED to act without direct instructions from the SCADA control center. SCADA systems are usually designed to be fault-tolerant systems with significant redundancy built into the system architecture.

Figure 2-2 shows the components and general configuration of a SCADA system. The control center houses a SCADA Server (MTU) and the communications routers. Other control center components include the HMI, engineering workstations, and the data historian, which are all connected by a LAN. The control center collects and logs information gathered by the field sites, displays information to the HMI, and may generate actions based upon detected events. The control center is also responsible for centralized alarming, trend analyses, and reporting. The field site performs local control of actuators and monitors sensors. Field sites are often equipped with a remote access capability to allow field operators to perform remote diagnostics and repairs usually over a separate dial up modem or WAN connection. Standard and proprietary communication protocols running over serial communications are used to transport information between the control center and field sites using telemetry techniques such as telephone line, cable, fiber, and radio frequency such as broadcast, microwave and satellite.

MTU-RTU communication architectures vary among implementations. The various architectures used, including point-to-point, series, series-star, and multi-drop [5], are shown in Figure 2-3. Point-to-point is functionally the simplest type; however, it is expensive because of the individual channels needed for each connection. In a series configuration, the number of channels used is reduced; however, channel sharing has an impact on the efficiency and complexity of SCADA operations. Similarly, the series-star and multi-drop configurations' use of one channel per device results in decreased efficiency and increased system complexity.

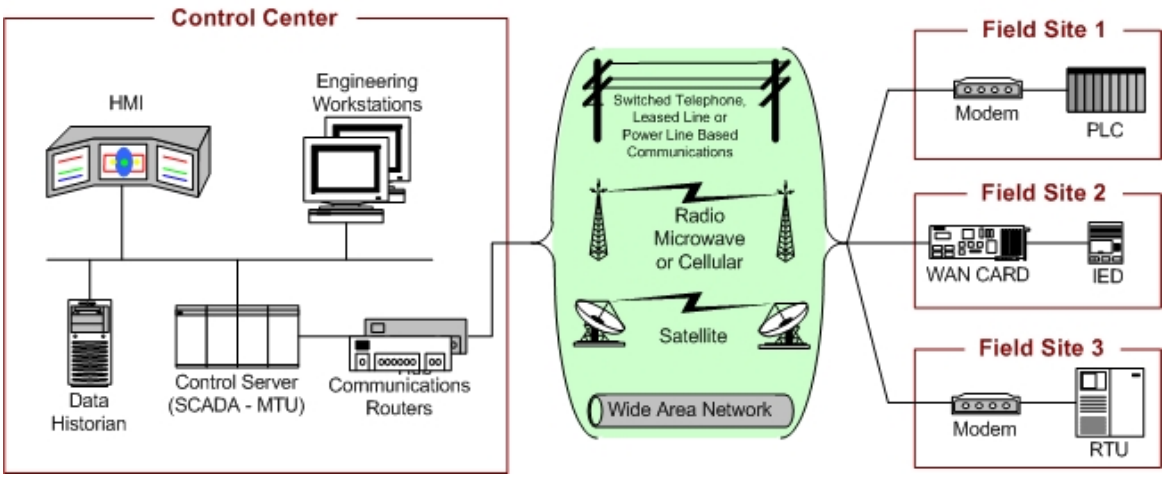

Figure 2-2. SCADA System General Layout

The four basic architectures shown in Figure 2-3 can be further augmented using dedicated communication devices to manage communication exchange as well as message switching and buffering. Large SCADA systems, containing hundreds of RTUs, often employ sub-MTUs to alleviate the burden on the primary MTU. This type of topology is shown in Figure 2-4.

Figure 2-5 shows an example of a SCADA system implementation. This particular SCADA system consists of a primary control center and three field sites. A second backup control center provides redundancy in the event of a primary control center malfunction. Point-to-point connections are used for all control center to field site communications, with two connections using radio telemetry. The third field site is local to the control center and uses the wide area network (WAN) for communications. A regional control center resides above the primary control center for a higher level of supervisory control. The corporate network has access to all control centers through the WAN, and field sites can be accessed remotely for troubleshooting and maintenance operations. The primary control center polls field devices for data at defined intervals (e.g., 5 seconds, 60 seconds) and can send new set points to a field device as required. In addition to polling and issuing high-level commands, the SCADA server also watches for priority interrupts coming from field site alarm systems.

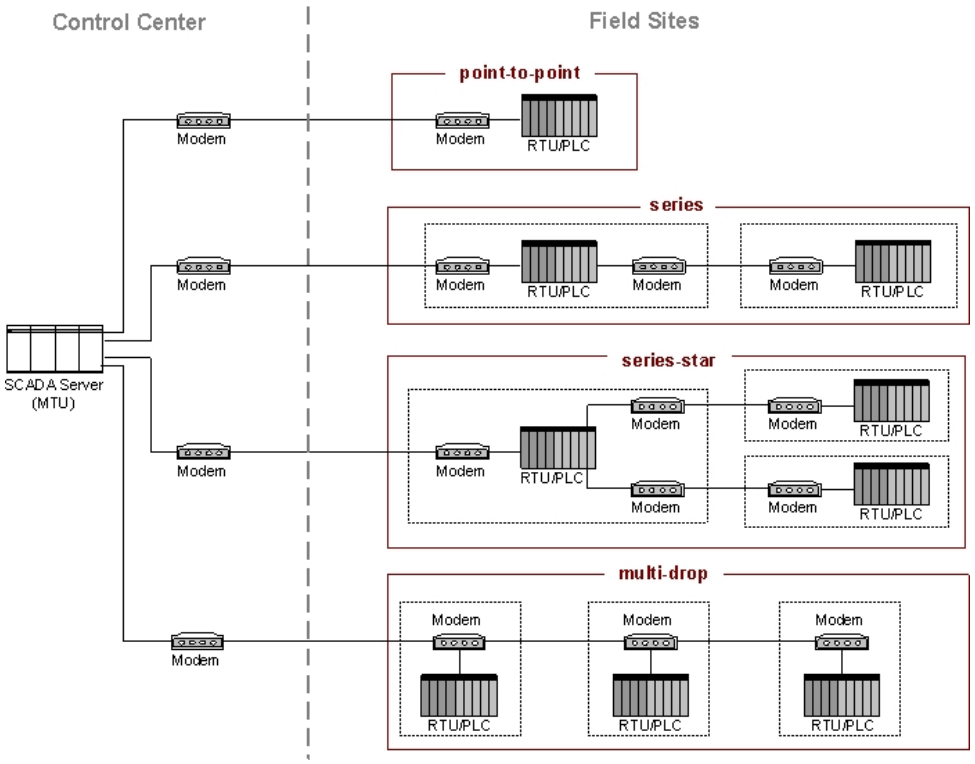

Figure 2-3. Basic SCADA Communication Topologies

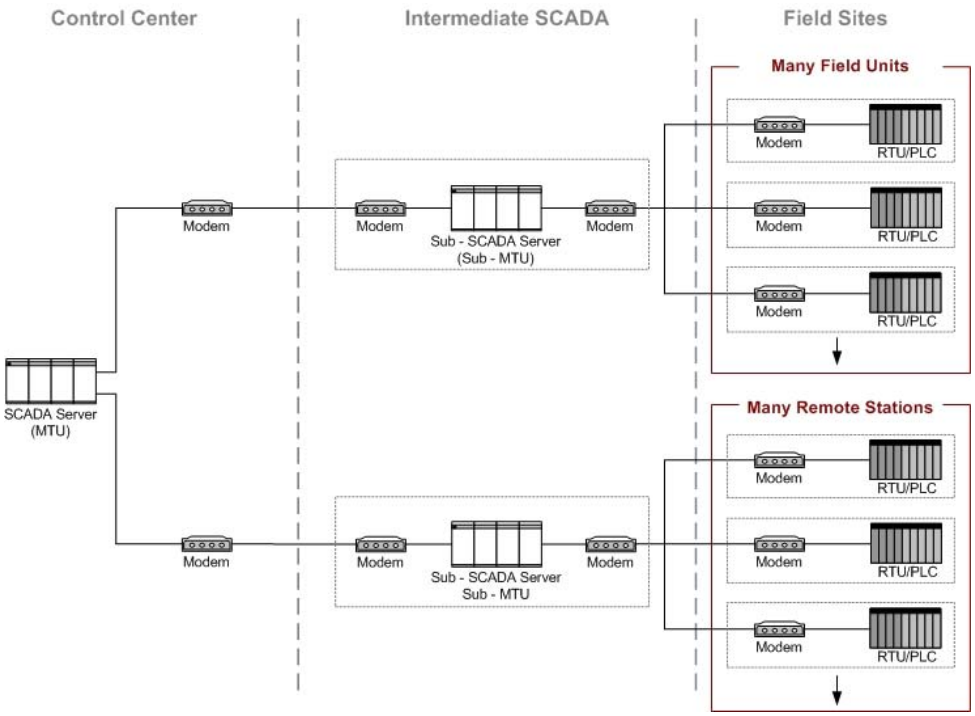

Figure 2-4. Large SCADA Communication Topology

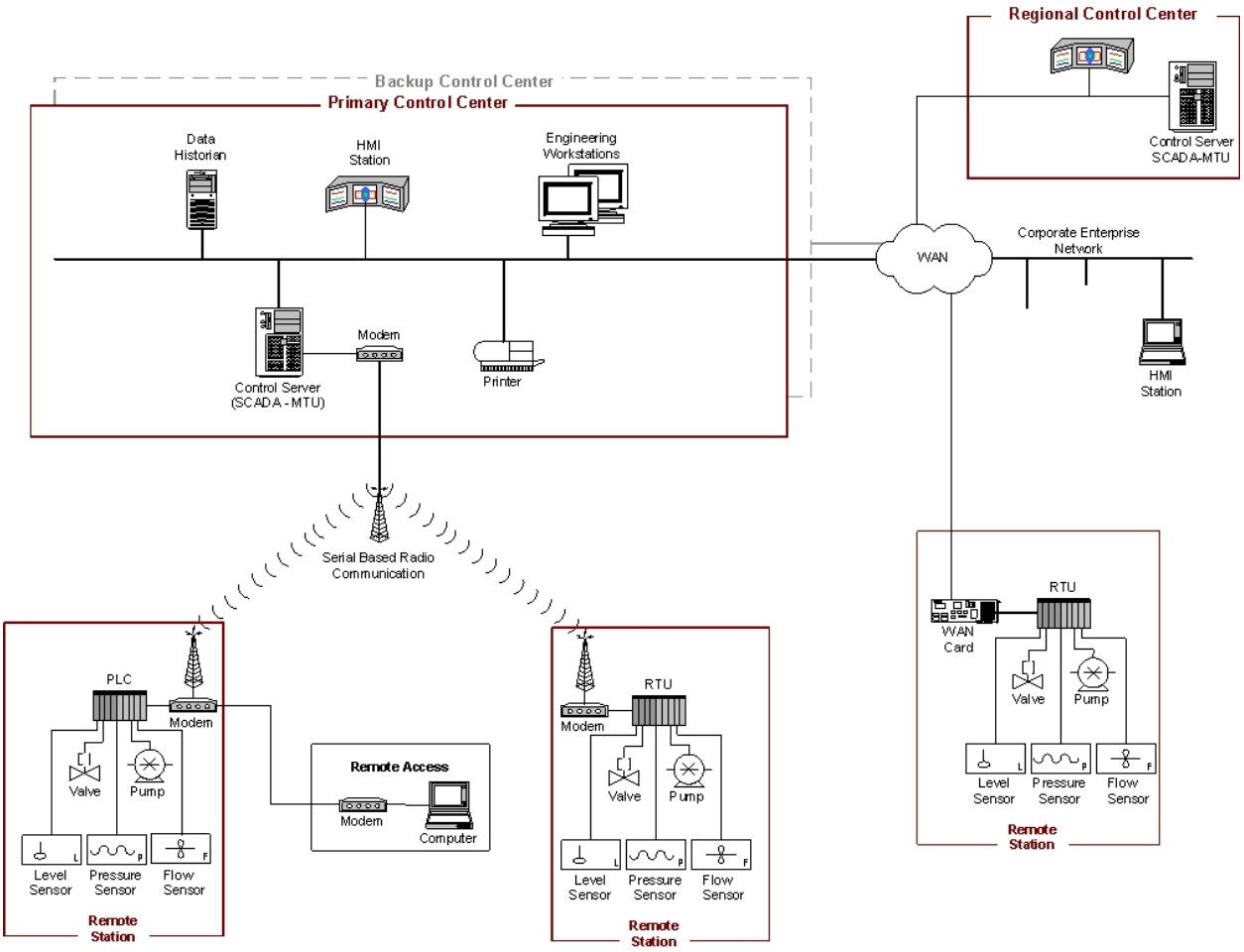

Figure 2-5. SCADA System Implementation Example (Distribution Monitoring and Control)

Figure 2-6 shows an example implementation for rail monitoring and control. This example includes a rail control center that houses the SCADA system and three sections of a rail system. The SCADA system polls the rail sections for information such as the status of the trains, signal systems, traction electrification systems, and ticket vending machines. This information is also fed to operator consoles at the HMI station within the rail control center. The SCADA system also monitors operator inputs at the rail control center and disperses high-level operator commands to the rail section components. In addition, the SCADA system monitors conditions at the individual rail sections and issues commands based on these conditions (e.g., shut down a train to prevent it from entering an area that has been determined to be flooded or occupied by another train based on condition monitoring).

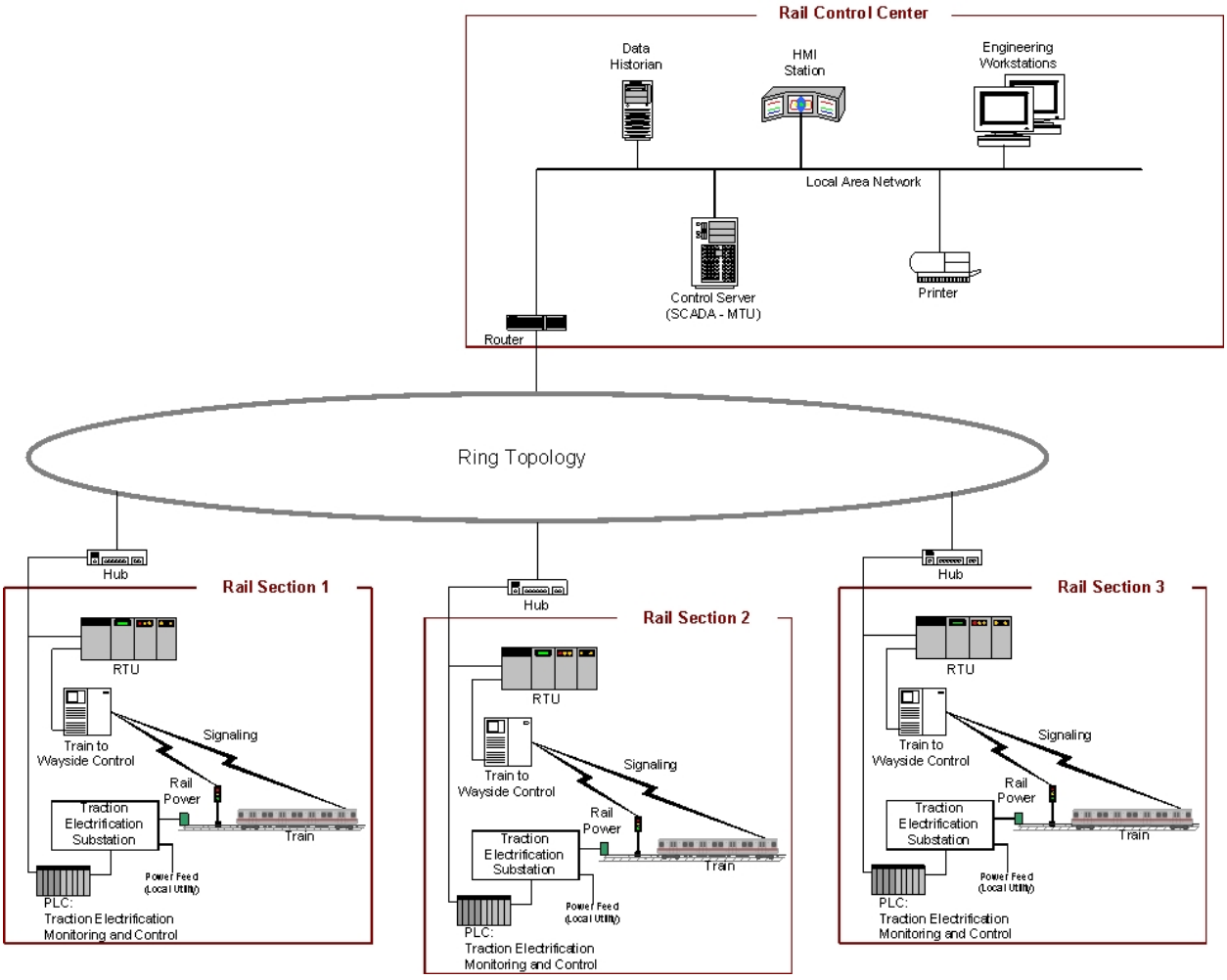

Figure 2-6. SCADA System Implementation Example (Rail Monitoring and Control)

2.5 Distributed Control Systems

DCS are used to control production systems within the same geographic location for industries such as oil refineries, water and wastewater treatment, electric power generation plants, chemical manufacturing plants, and pharmaceutical processing facilities. These systems are usually process control or discrete part control systems. A DCS uses a centralized supervisory control loop to mediate a group of localized controllers that share the overall tasks of carrying out an entire production process [6]. By modularizing the production system, a DCS reduces the impact of a single fault on the overall system. In many modern systems, the DCS is interfaced with the corporate network to give business operations a view of production.

An example implementation showing the components and general configuration of a DCS is depicted in Figure 2-7. This DCS encompasses an entire facility from the bottom-level production processes up to the corporate or enterprise layer. In this example, a supervisory controller (control server) communicates to its subordinates via a control network. The supervisor sends set points to and requests data from the distributed field controllers. The distributed controllers control their process actuators based on control server commands and sensor feedback from process sensors.

Figure 2-7 gives examples of low-level controllers found on a DCS system. The field control devices shown include a PLC, a process controller, a single loop controller, and a machine controller. The single loop controller interfaces sensors and actuators using point-to-point wiring, while the other three field devices incorporate fieldbus networks to interface with process sensors and actuators. Fieldbus networks eliminate the need for point-to-point wiring between a controller and individual field sensors and actuators. Additionally, a fieldbus allows greater functionality beyond control, including field device diagnostics, and can accomplish control algorithms within the fieldbus, thereby avoiding signal routing back to the PLC for every control operation. Standard industrial communication protocols designed by industry groups such as Modbus and Fieldbus [7] are often used on control networks and fieldbus networks.

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

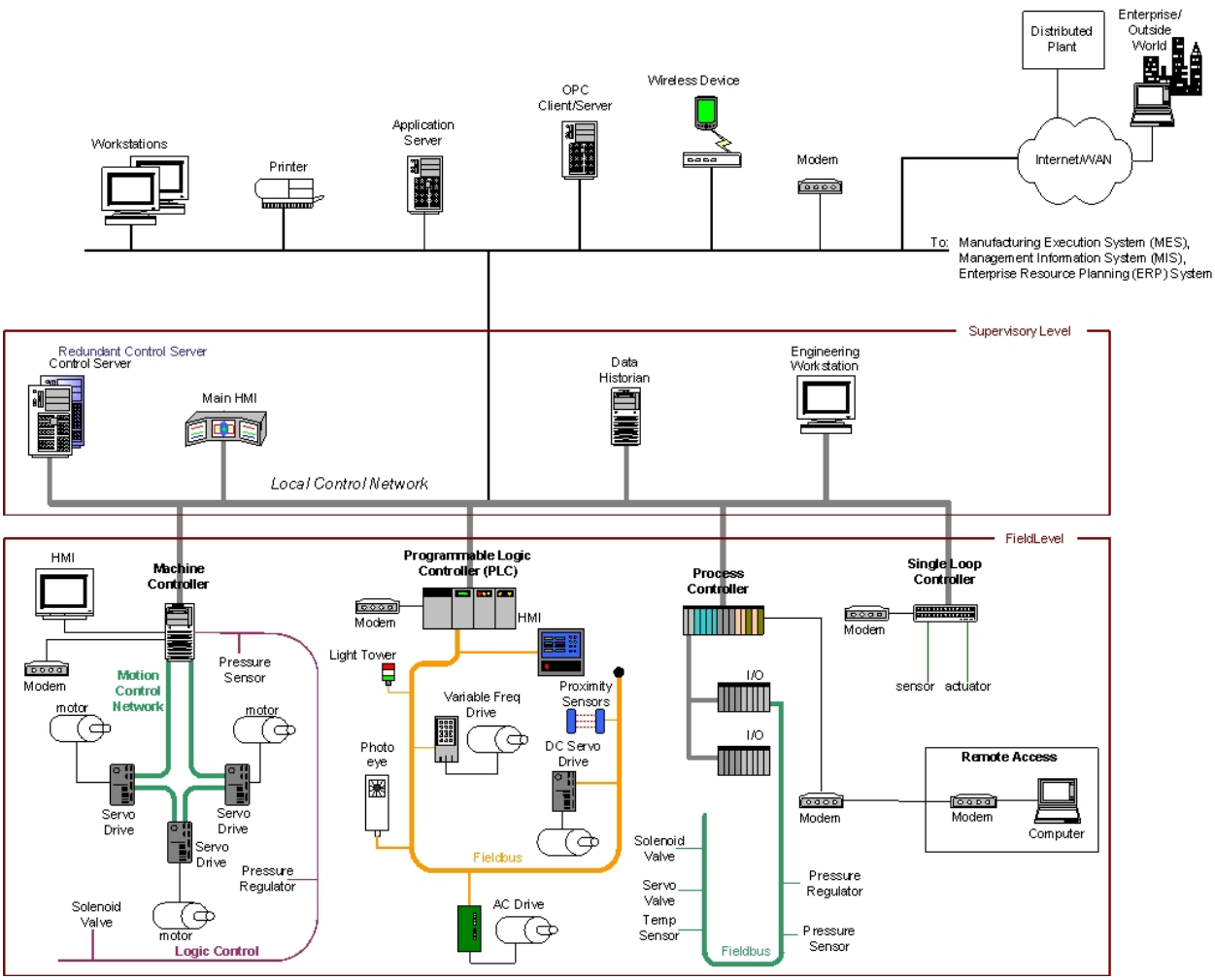

Figure 2-7. DCS Implementation Example

2.6 Programmable Logic Controllers

PLCs are used in both SCADA and DCS systems as the control components of an overall hierarchical system to provide local management of processes through feedback control as described in the sections above. In the case of SCADA systems, they provide the same functionality of RTUs. When used in DCS, PLCs are implemented as local controllers within a supervisory control scheme. PLCs are also implemented as the primary components in smaller control system configurations. PLCs have a user-programmable memory for storing instructions for the purpose of implementing specific functions such as I/O control, logic, timing, counting, three mode proportional-integral-derivative (PID) control, communication, arithmetic, and data and file processing. Figure 2-8 shows control of a manufacturing process being performed by a PLC over a fieldbus network. The PLC is accessible via a programming interface located on an engineering workstation, and data is stored in a data historian, all connected on a LAN.

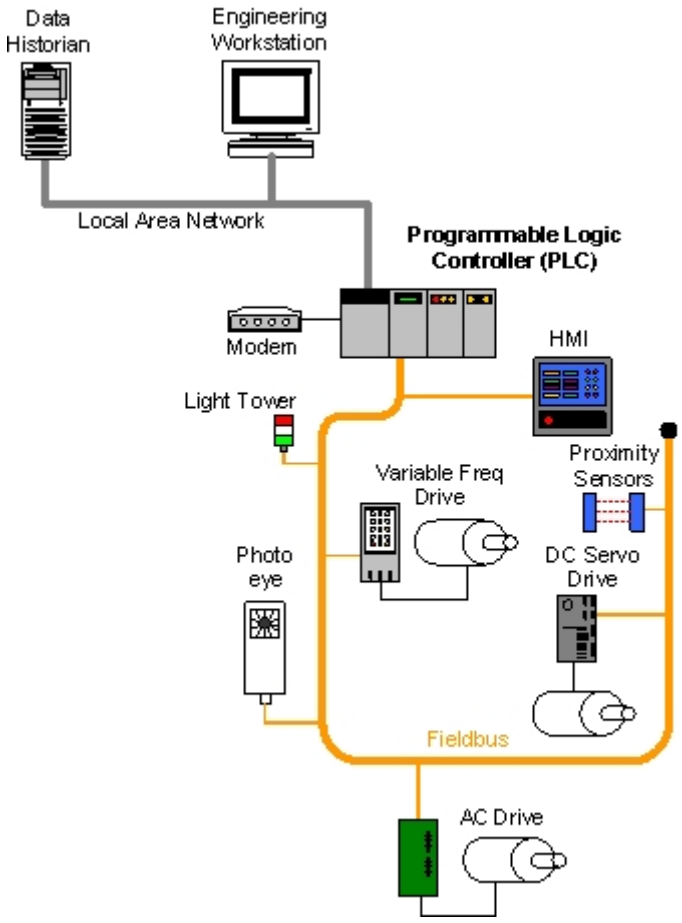

Figure 2-8. PLC Control System Implementation Example

2.7 Industrial Sectors and Their Interdependencies

Both the electrical power transmission and distribution grid industries use geographically distributed SCADA control technology to operate highly interconnected and dynamic systems consisting of thousands of public and private utilities and rural cooperatives for supplying electricity to end users. SCADA systems monitor and control electricity distribution by collecting data from and issuing commands to geographically remote field control stations from a centralized location. SCADA systems are also used to monitor and control water, oil and natural gas distribution, including pipelines, ships, trucks, and rail systems, as well as wastewater collection systems.

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

The U.S. critical infrastructure is often referred to as a "system of systems" because of the interdependencies that exist between its various industrial sectors as well as interconnections between business partners [8] [9]. Critical infrastructures are highly interconnected and mutually dependent in complex ways, both physically and through a host of information and communications technologies. An incident in one infrastructure can directly and indirectly affect other infrastructures through cascading and escalating failures.

Electric power is often thought to be one of the most prevalent sources of disruptions of interdependent critical infrastructures. As an example, a cascading failure can be initiated by a disruption of the microwave communications network used for an electric power transmission SCADA system. The lack of monitoring and control capabilities could cause a large generating unit to be taken offline, an event that would lead to loss of power at a transmission substation. This loss could cause a major imbalance, triggering a cascading failure across the power grid. This could result in large area blackouts that could potentially affect oil and natural gas production, refinery operations, water treatment systems, wastewater collection systems, and pipeline transport systems that rely on the grid for electric power.

3. ICS Characteristics, Threats and Vulnerabilities

Most ICS in use today were developed years ago, long before public and private networks, desktop computing, or the Internet were a common part of business operations. These systems were designed to meet performance, reliability, safety, and flexibility requirements. In most cases they were physically isolated from outside networks and based on proprietary hardware, software, and communication protocols that included basic error detection and correction capabilities, but lacked the secure communication capabilities required in today's interconnected systems. While there was concern for Reliability, Maintainability, and Availability (RMA) when addressing statistical performance and failure, the need for cyber security measures within these systems was not anticipated. At the time, security for ICS meant physically securing access to the network and the consoles that controlled the systems.

ICS development paralleled the evolution of microprocessor, personal computer, and networking technologies during the 1980's and 1990's, and Internet-based technologies started making their way into ICS designs in the late 1990's. These changes to ICS exposed them to new types of threats and significantly increased the likelihood that ICS could be compromised. This section describes the unique security characteristics of ICS, the vulnerabilities in ICS implementations, and the threats and incidents that ICS may face. Section 3.7 presents several examples of actual ICS cyber security incidents.

3.1 Comparing ICS and IT Systems

Initially, ICS had little resemblance to IT systems in that ICS were isolated systems running proprietary control protocols using specialized hardware and software. Widely available, low-cost Internet Protocol (IP) devices are now replacing proprietary solutions, which increases the possibility of cyber security vulnerabilities and incidents. As ICS are adopting IT solutions to promote corporate connectivity and remote access capabilities, and are being designed and implemented using industry standard computers, operating systems (OS) and network protocols, they are starting to resemble IT systems. This integration supports new IT capabilities, but it provides significantly less isolation for ICS from the outside world than predecessor systems, creating a greater need to secure these systems. While security solutions have been designed to deal with these security issues in typical IT systems, special precautions must be taken when introducing these same solutions to ICS environments. In some cases, new security solutions are needed that are tailored to the ICS environment.

ICS have many characteristics that differ from traditional IT systems, including different risks and priorities. Some of these include significant risk to the health and safety of human lives, serious damage to the environment, and financial issues such as production losses, and negative impact to a nation's economy. ICS have different performance and reliability requirements and use operating systems and applications that may be considered unconventional to typical IT support personnel. Furthermore, the goals of safety and efficiency can sometimes conflict with security in the design and operation of control systems (e.g., requiring password authentication and authorization should not hamper or interfere with emergency actions for ICS.) The following lists some special considerations when considering security for ICS:

- **Performance Requirements.** ICS are generally time-critical, with the criterion for acceptable levels of delay and jitter dictated by the individual installation. Some systems require deterministic responses. High throughput is typically not essential to ICS. In contrast, IT systems typically require high throughput, and they can typically withstand some level of delay and jitter

- **Availability Requirements.** Many ICS processes are continuous in nature. Unexpected outages of systems that control industrial processes are not acceptable. Outages often must be planned and scheduled days/weeks in advance. Exhaustive pre-deployment testing is essential to ensure high

availability for the ICS. In addition to unexpected outages, many control systems cannot be easily stopped and started without affecting production. In some cases, the products being produced or equipment being used is more important than the information being relayed. Therefore, the use of typical IT strategies such as rebooting a component, are usually not acceptable solutions due to the adverse impact on the requirements for high availability, reliability and maintainability of the ICS. Some ICS employ redundant components, often running in parallel, to provide continuity when primary components are unavailable.

- **Risk Management Requirements.** In a typical IT system, data confidentiality and integrity are typically the primary concerns. For an ICS, human safety and fault tolerance to prevent loss of life or endangerment of public health or confidence, regulatory compliance, loss of equipment, loss of intellectual property, or lost or damaged products are the primary concerns. The personnel responsible for operating, securing, and maintaining ICS must understand the important link between safety and security.

- **Architecture Security Focus.** In a typical IT system, the primary focus of security is protecting the operation of IT assets, whether centralized or distributed, and the information stored on or transmitted among these assets. In some architectures, information stored and processed centrally is more critical and is afforded more protection. For ICS, edge clients (e.g., PLC, operator station, DCS controller) need to be carefully protected because they are directly responsible for controlling the end processes. The protection of the central server is still very important in an ICS, because the central server could possibly adversely impact every edge device.

- **Physical Interaction.** In a typical IT system, there is not physical interaction with the environment. ICS can have very complex interactions with physical processes and consequences in the ICS domain that can manifest in physical events. All security functions integrated into the ICS must be tested (e.g., off-line on a comparable ICS) to prove that they do not compromise normal ICS functionality.

- **Time-Critical Responses.** In a typical IT system, access control can be implemented without significant regard for data flow. For some ICS, automated response time or system response to human interaction is very critical. For example, requiring password authentication and authorization on an HMI must not hamper or interfere with emergency actions for ICS. Information flow must not be interrupted or compromised. Access to these systems should be restricted by rigorous physical security controls.

- **System Operation.** ICS operating systems (OS) and applications may not tolerate typical IT security practices. Legacy systems are especially vulnerable to resource unavailability and timing disruptions. Control networks are often more complex and require a different level of expertise (e.g., control networks are typically managed by control engineers, not IT personnel). Software and hardware are more difficult to upgrade in an operational control system network. Many systems may not have desired features including encryption capabilities, error logging, and password protection.

- **Resource Constraints.** ICS and their real time OSs are often resource-constrained systems that usually do not include typical IT security capabilities. There may not be computing resources available on ICS components to retrofit these systems with current security capabilities. Additionally, in some instances, third-party security solutions are not allowed due to ICS vendor license and service agreements, and loss of service support can occur if third party applications are installed without vendor acknowledgement or approval.

- **Communications.** Communication protocols and media used by ICS environments for field device control and intra-processor communication are typically different from the generic IT environment, and may be proprietary.

- **Change Management.** Change management is paramount to maintaining the integrity of both IT and control systems. Unpatched software represents one of the greatest vulnerabilities to a system. Software updates on IT systems, including security patches, are typically applied in a timely fashion based on appropriate security policy and procedures. In addition, these procedures are often automated using server-based tools. Software updates on ICS cannot always be implemented on a timely basis because these updates need to be thoroughly tested by the vendor of the industrial control application and the end user of the application before being implemented and ICS outages often must be planned and scheduled days/weeks in advance. The ICS may also require revalidation as part of the update process. Another issue is that many ICS utilize older versions of operating systems that are no longer supported by the vendor. Consequently, available patches may not be applicable. Change management is also applicable to hardware and firmware. The change management process, when applied to ICS, requires careful assessment by ICS experts (e.g., control engineers) working in conjunction with security and IT personnel.

- **Managed Support.** Typical IT systems allow for diversified support styles, perhaps supporting disparate but interconnected technology architectures. For ICS, service support is usually via a single vendor, which may not have a diversified and interoperable support solution from another vendor.

- **Component Lifetime.** Typical IT components have a lifetime on the order of 3 to 5 years, with brevity due to the quick evolution of technology. For ICS where technology has been developed in many cases for very specific use and implementation, the lifetime of the deployed technology is often in the order of 15 to 20 years and sometimes longer.

- **Access to Components**. Typical IT components are usually local and easy to access, while ICS components can be isolated, remote, and require extensive physical effort to gain access to them.

Table 3-1 summarizes some of the typical differences between IT systems and ICS.

Table 3-1. Summary of IT System and ICS Differences

Category	Information Technology System	Industrial Control System
Performance Requirements	Non-real-time Response must be consistent High throughput is demanded High delay and jitter may be acceptable	Real-time Response is time-critical Modest throughput is acceptable High delay and/or jitter is not acceptable
Availability Requirements	Responses such as rebooting are acceptable Availability deficiencies can often be tolerated, depending on the system's operational requirements	Responses such as rebooting may not be acceptable because of process availability requirements Availability requirements may necessitate redundant systems Outages must be planned and scheduled days/weeks in advance High availability requires exhaustive pre-deployment testing

Category	Information Technology System	Industrial Control System
Risk Management Requirements	Data confidentiality and integrity is paramount Fault tolerance is less important – momentary downtime is not a major risk Major risk impact is delay of business operations	Human safety is paramount, followed by protection of the process Fault tolerance is essential, even momentary downtime may not be acceptable Major risk impacts are regulatory non-compliance, environmental impacts, loss of life, equipment, or production
Architecture Security Focus	Primary focus is protecting the IT assets, and the information stored on or transmitted among these assets. Central server may require more protection	Primary goal is to protect edge clients (e.g., field devices such as process controllers) Protection of central server is also important
Unintended Consequences	Security solutions are designed around typical IT systems	Security tools must be tested (e.g., off-line on a comparable ICS) to ensure that they do not compromise normal ICS operation
Time-Critical Interaction	Less critical emergency interaction Tightly restricted access control can be implemented to the degree necessary for security	Response to human and other emergency interaction is critical Access to ICS should be strictly controlled, but should not hamper or interfere with human-machine interaction
System Operation	Systems are designed for use with typical operating systems Upgrades are straightforward with the availability of automated deployment tools	Differing and possibly proprietary operating systems, often without security capabilities built in Software changes must be carefully made, usually by software vendors, because of the specialized control algorithms and perhaps modified hardware and software involved
Resource Constraints	Systems are specified with enough resources to support the addition of third-party applications such as security solutions	Systems are designed to support the intended industrial process and may not have enough memory and computing resources to support the addition of security capabilities
Communications	Standard communications protocols Primarily wired networks with some localized wireless capabilities Typical IT networking practices	Many proprietary and standard communication protocols Several types of communications media used including dedicated wire and wireless (radio and satellite) Networks are complex and sometimes require the expertise of control engineers
Change Management	Software changes are applied in a timely fashion in the presence of good security policy and procedures. The procedures are often automated.	Software changes must be thoroughly tested and deployed incrementally throughout a system to ensure that the integrity of the control system is maintained. ICS outages often must be planned and scheduled days/weeks in advance. ICS may use OSs that are no longer supported
Managed Support	Allow for diversified support styles	Service support is usually via a single vendor
Component Lifetime	Lifetime on the order of 3-5 years	Lifetime on the order of 15-20 years
Access to Components	Components are usually local and easy to access	Components can be isolated, remote, and require extensive physical effort to gain access to them

Available computing resources for ICS (including central processing unit [CPU] time and memory) tend to be very limited because these systems were designed to maximize control system resources, with little to no extra capacity for third-party cyber security solutions. Additionally, in some instances, third-party security solutions are not allowed due to vendor license and service agreements, and loss of service support can occur if third party applications are installed. Another important consideration is that IT cyber security and control systems expertise is typically not found within the same group of personnel.

In summary, the operational and risk differences between ICS and IT systems create the need for increased sophistication in applying cyber security and operational strategies. A cross-functional team of control engineers, control system operators and IT security professionals needs to work closely to understand the possible implications of the installation, operation, and maintenance of security solutions in conjunction with control system operation. IT professionals working with ICS need to understand the reliability impacts of information security technologies before deployment. Some of the OSs and applications running on ICS may not operate correctly with commercial-off-the-shelf (COTS) IT cyber security solutions because of specialized ICS environment architectures.

3.2 Threats

Threats to control systems can come from numerous sources, including adversarial sources such as hostile governments, terrorist groups, industrial spies, disgruntled employees, malicious intruders, and natural sources such as from system complexities, human errors and accidents, equipment failures and natural disasters. To protect against adversarial threats (as well as known natural threats), it is necessary to create a defense-in-depth strategy for the ICS. Table 3-2 lists possible threats to ICS. Please note this list is in alphabetical order and not by greatest threat.

Table 3-2. Adversarial Threats to ICS

Threat Agent	Description
Attackers	Attackers break into networks for the thrill of the challenge or for bragging rights in the attacker community. While remote cracking once required a fair amount of skill or computer knowledge, attackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. Many attackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of attackers poses a relatively high threat of an isolated or brief disruption causing serious damage.
Bot-network operators	Bot-network operators are attackers; however, instead of breaking into systems for the challenge or bragging rights, they take over multiple systems to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of compromised systems and networks are sometimes made available on underground markets (e.g., purchasing a denial of service attack or the use of servers to relay spam or phishing attacks).
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized crime groups are using spam, phishing, and spyware/malware to commit identity theft and online fraud. International corporate spies and organized crime organizations also pose a threat to the U.S. through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop attacker talent. Some criminal groups may try to extort money from an organization by threatening a cyber attack.

Threat Agent	Description
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrines, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power – impacts that could affect the daily lives of U.S. citizens.
Insiders	The disgruntled insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors as well as employees who accidentally introduce malware into systems. Insiders may be employees, contractors, or business partners. Inadequate policies, procedures, and testing can, and have led to ICS impacts. Impacts have ranged from trivial to significant damage to the ICS and field devices. Unintentional impacts from insiders are some of the highest probability occurrences.
Phishers	Phishers are individuals or small groups that execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware/malware to accomplish their objectives.
Spammers	Spammers are individuals or organizations that distribute unsolicited e-mail with hidden or false information to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations (e.g., DoS).
Spyware/malware authors	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware to generate funds or gather sensitive information. Terrorists may attack one target to divert attention or resources from other targets.
Industrial spies	Industrial espionage seeks to acquire intellectual property and know-how by clandestine methods

Source: Government Accountability Office (GAO), Department of Homeland Security's (DHS's) Role in Critical Infrastructure Protection (CIP) Cybersecurity, GAO-05-434 (Washington, D.C.: May, 2005).

3.3 Potential ICS Vulnerabilities

This section lists vulnerabilities that may be found in typical ICS. The order of these vulnerabilities does not necessarily reflect any priority in terms of likelihood of occurrence or severity of impact. The vulnerabilities are grouped into Policy and Procedure, Platform, and Network categories to assist in determining optimal mitigation strategies. Any given ICS will usually exhibit a subset of these vulnerabilities, but may also contain additional vulnerabilities unique to the particular ICS implementation that do not appear in this listing. Specific information on ICS vulnerabilities can be researched at the United States Computer Emergency Readiness Team (US-CERT) Control Systems Web site.[2]

When studying possible security vulnerabilities, it is easy to become preoccupied with trying to address issues that are technically interesting, but are ultimately of low impact. As addressed in Appendix E,

[2] The US-CERT Control Systems Web site is located at http://www.us-cert.gov/control_systems/.

FIPS 199 establishes security categories for both information and information systems based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals.

A method for assessing and rating the risk of a possible vulnerability at a specific facility is needed. The risk is a function of the likelihood (probability) that a defined threat agent (adversary) can exploit a specific vulnerability and create an impact (consequence). The risk induced by any given vulnerability is influenced by a number of related indicators, including:

- Network and computer architecture and conditions
- Installed countermeasures
- Technical difficulty of the attack
- Probability of detection (e.g., amount of time the adversary can remain in contact with the target system/network without detection)
- Consequences of the incident
- Cost of the incident.

This assessment of risk is addressed in further detail in Sections 4 through 6.

3.3.1 Policy and Procedure Vulnerabilities

Vulnerabilities are often introduced into ICS because of incomplete, inappropriate, or nonexistent security documentation, including policy and implementation guides (procedures). Security documentation, along with management support, is the cornerstone of any security program. Corporate security policy can reduce vulnerabilities by mandating conduct such as password usage and maintenance or requirements for connecting modems to ICS. Table 3-3 describes potential policy and procedure vulnerabilities for ICS.

Table 3-3. Policy and Procedure Vulnerabilities

Vulnerability	Description
Inadequate security policy for the ICS	Vulnerabilities are often introduced into ICS due to inadequate policies or the lack of policies specifically for control system security.
No formal ICS security training and awareness program	A documented formal security training and awareness program is designed to keep staff up to date on organizational security policies and procedures as well as industry cyber security standards and recommended practices. Without training on specific ICS policies and procedures, staff cannot be expected to maintain a secure ICS environment.
Inadequate security architecture and design	Control engineers have historically had minimal training in security and until relatively recently vendors have not included security features in their products
No specific or documented security procedures were developed from the security policy for the ICS	Specific security procedures should be developed and employees trained for the ICS. They are the roots of a sound security program.
Absent or deficient ICS equipment implementation guidelines	Equipment implementation guidelines should be kept up to date and readily available. These guidelines are an integral part of security procedures in the event of an ICS malfunction.
Lack of administrative mechanisms for security enforcement	Staff responsible for enforcing security should be held accountable for administering documented security policies and procedures.

Vulnerability	Description
Few or no security audits on the ICS	Independent security audits should review and examine a system's records and activities to determine the adequacy of system controls and ensure compliance with established ICS security policy and procedures. Audits should also be used to detect breaches in ICS security services and recommend changes, which may include making existing security controls more robust and/or adding new security controls.
No ICS specific continuity of operations or disaster recovery plan (DRP)	A DRP should be prepared, tested and available in the event of a major hardware or software failure or destruction of facilities. Lack of a specific DRP for the ICS could lead to extended downtimes and production loss.
Lack of ICS specific configuration change management	A process for controlling modifications to hardware, firmware, software, and documentation should be implemented to ensure an ICS is protected against inadequate or improper modifications before, during, and after system implementation. A lack of configuration change management procedures can lead to security oversights, exposures, and risks.

3.3.2 Platform Vulnerabilities

Vulnerabilities in ICS can occur due to flaws, misconfigurations, or poor maintenance of their platforms, including hardware, operating systems, and ICS applications. These vulnerabilities can be mitigated through various security controls, such as OS and application patching, physical access control, and security software (e.g., antivirus software). The tables in this section describe potential platform vulnerabilities:

- Table 3-4. Platform Configuration Vulnerabilities
- Table 3-5. Platform Hardware Vulnerabilities
- Table 3-6. Platform Software Vulnerabilities
- Table 3-7. Platform Malware Protection Vulnerabilities

Table 3-4. Platform Configuration Vulnerabilities

Vulnerability	Description
OS and vendor software patches may not be developed until significantly after security vulnerabilities are found	Because of the complexity of ICS software and possible modifications to the underlying OS, changes must undergo comprehensive regression testing. The elapsed time for such testing and subsequent distribution of updated software provides a long window of vulnerability
OS and application security patches are not maintained	Out-of-date OSs and applications may contain newly discovered vulnerabilities that could be exploited. Documented procedures should be developed for how security patches will be maintained. Security patch support may not even be available for ICS that use outdated OSs.
OS and application security patches are implemented without exhaustive testing	OS and application security patches deployed without testing could compromise normal operation of the ICS. Documented procedures should be developed for testing new security patches.
Default configurations are used	Using default configurations often leads to insecure and unnecessary open ports and exploitable services and applications running on hosts.
Critical configurations are not stored or backed up	Procedures should be available for restoring ICS configuration settings in the event of accidental or adversary-initiated configuration changes to maintain system availability and prevent loss of data. Documented procedures should be developed for maintaining ICS configuration settings.

Vulnerability	Description
Data unprotected on portable device	If sensitive data (e.g., passwords, dial-up numbers) is stored in the clear on portable devices such as laptops and PDAs and these devices are lost or stolen, system security could be compromised. Policy, procedures, and mechanisms are required for protection.
Lack of adequate password policy	Password policies are needed to define when passwords must be used, how strong they must be, and how they must be maintained. Without a password policy, systems might not have appropriate password controls, making unauthorized access to systems more likely. Password policies should be developed as part of an overall ICS security program taking into account the capabilities of the ICS and its personnel to handle more complex passwords.
No password used	Passwords should be implemented on ICS components to prevent unauthorized access. Password-related vulnerabilities include having no password for: • System login (if the system has user accounts) • System power-on (if the system has no user accounts) • System screen saver (if an ICS component is unattended over time) Password authentication should not hamper or interfere with emergency actions for ICS.
Password disclosure	Passwords should be kept confidential to prevent unauthorized access. Examples of password disclosures include: • Posting passwords in plain sight, local to a system • Sharing passwords to individual user accounts with associates • Communicating passwords to adversaries through social engineering • Sending passwords that are not encrypted through unprotected communications
Password guessing	Poorly chosen passwords can easily be guessed by humans or computer algorithms to gain unauthorized access. Examples include: • Passwords that are short, simple (e.g., all lower-case letters), or otherwise do not meet typical strength requirements. Password strength also depends on the specific ICS capability to handle more stringent passwords • Passwords that are left as the default vendor supplied value • Passwords that are not changed on a specified interval
Inadequate access controls applied	Poorly specified access controls can result in giving an ICS user too many or too few privileges. The following exemplify each case: • System configured with default access control settings gives an operator administrative privileges • System improperly configured results in an operator being unable to take corrective actions in an emergency situation Access control policies should be developed as part of an ICS security program.

Table 3-5. Platform Hardware Vulnerabilities

Vulnerability	Description
Inadequate testing of security changes	Many ICS facilities, especially smaller facilities, have no test facilities, so security changes must be implemented using the live operational systems
Inadequate physical protection for critical systems	Access to the control center, field devices, portable devices, media, and other ICS components needs to be controlled. Many remote sites are often not staffed and it may not be feasible to physically monitor them.
Unauthorized personnel have physical access to equipment	Physical access to ICS equipment should be restricted to only the necessary personnel, taking into account safety requirements, such as emergency shutdown or restarts. Improper access to ICS equipment can lead to any of the following: • Physical theft of data and hardware • Physical damage or destruction of data and hardware • Unauthorized changes to the functional environment (e.g., data connections, unauthorized use of removable media, adding/removing resources) • Disconnection of physical data links • Undetectable interception of data (keystroke and other input logging)
Insecure remote access on ICS components	Modems and other remote access capabilities that enable control engineers and vendors to gain remote access to systems should be deployed with security controls to prevent unauthorized individuals from gaining access to the ICS.
Dual network interface cards (NIC) to connect networks	Machines with dual NICs connected to different networks could allow unauthorized access and passing of data from one network to another.
Undocumented assets	To properly secure an ICS, there should be an accurate listing of the assets in the system. An inaccurate representation of the control system and its components could leave an unauthorized access point or backdoor into the ICS.
Radio frequency and electro-magnetic pulse (EMP)	The hardware used for control systems is vulnerable to radio frequency and electro-magnetic pulses (EMP). The impact can range from temporary disruption of command and control to permanent damage to circuit boards.
Lack of backup power	Without backup power to critical assets, a general loss of power will shut down the ICS and could create an unsafe situation. Loss of power could also lead to insecure default settings.
Loss of environmental control	Loss of environmental control could lead to processors overheating. Some processors will shut down to protect themselves; some may continue to operate but in a minimal capacity, producing intermittent errors; and some just melt if they overheat.
Lack of redundancy for critical components	Lack of redundancy in critical components could provide single point of failure possibilities

Table 3-6. Platform Software Vulnerabilities

Vulnerability	Description
Buffer overflow	Software used to implement an ICS could be vulnerable to buffer overflows; adversaries could exploit these to perform various attacks.
Installed security capabilities not enabled by default	Security capabilities that were installed with the product are useless if they are not enabled or at least identified as being disabled.
Denial of service (DoS)	ICS software could be vulnerable to DoS attacks, resulting in the prevention of authorized access to a system resource or delaying system operations and functions.

Vulnerability	Description
Mishandling of undefined, poorly defined, or “illegal” conditions	Some ICS implementations are vulnerable to packets that are malformed or contain illegal or otherwise unexpected field values.
OLE for Process Control (OPC) relies on Remote Procedure Call (RPC) and Distributed Component Object Model (DCOM)	Without updated patches, OPC is vulnerable to the known RPC/DCOM vulnerabilities.
Use of insecure industry-wide ICS protocols	Distributed Network Protocol (DNP) 3.0, Modbus, Profibus, and other protocols are common across several industries and protocol information is freely available. These protocols often have few or no security capabilities built in.
Use of clear text	Many ICS protocols transmit messages in clear text across the transmission media, making them susceptible to eavesdropping by adversaries.
Unneeded services running	Many platforms have a wide variety of processor and network services defined to operate as a default. Unneeded services are seldom disabled and could be exploited.
Use of proprietary software that has been discussed at conferences and in periodicals	Proprietary software issues are discussed at international IT, ICS and “Black Hat” conferences and available through technical papers, periodicals and listservers. Also, ICS maintenance manuals are available from the vendors. This information can help adversaries create successful attacks against ICS.
Inadequate authentication and access control for configuration and programming software	Unauthorized access to configuration and programming software could provide the ability to corrupt a device.
Intrusion detection/prevention software not installed	Incidents can result in loss of system availability; the capture, modification, and deletion of data; and incorrect execution of control commands. IDS/IPS software may stop or prevent various types of attacks, including DoS attacks, and also identify attacked internal hosts, such as those infected with worms. IDS/IPS software must be tested prior to deployment to determine that it does not compromise normal operation of the ICS.
Logs not maintained	Without proper and accurate logs, it might be impossible to determine what caused a security event to occur.
Incidents are not detected	Where logs and other security sensors are installed, they may not be monitored on a real-time basis and therefore security incidents may not be rapidly detected and countered.

Table 3-7. Platform Malware Protection Vulnerabilities

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

3.3.3 Network Vulnerabilities

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

The tables in this section describe potential platform vulnerabilities:

- Table 3-8. Network Configuration Vulnerabilities
- Table 3-9. Network Hardware Vulnerabilities
- Table 3-10. Network Perimeter Vulnerabilities
- Table 3-11. Network Monitoring and Logging Vulnerabilities
- Table 3-12. Communication Vulnerabilities
- Table 3-13. Wireless Connection Vulnerabilities

Table 3-8. Network Configuration Vulnerabilities

Vulnerability	Description
Weak network security architecture	The network infrastructure environment within the ICS has often been developed and modified based on business and operational requirements, with little consideration for the potential security impacts of the changes. Over time, security gaps may have been inadvertently introduced within particular portions of the infrastructure. Without remediation, these gaps may represent backdoors into the ICS.
Data flow controls not employed	Data flow controls, such as access control lists (ACL), are needed to restrict which systems can directly access network devices. Generally, only designated network administrators should be able to access such devices directly. Data flow controls should ensure that other systems cannot directly access the devices.
Poorly configured security equipment	Using default configurations often leads to insecure and unnecessary open ports and exploitable network services running on hosts. Improperly configured firewall rules and router ACLs can allow unnecessary traffic.
Network device configurations not stored or backed up	Procedures should be available for restoring network device configuration settings in the event of accidental or adversary-initiated configuration changes to maintain system availability and prevent loss of data. Documented procedures should be developed for maintaining network device configuration settings.
Passwords are not encrypted in transit	Passwords transmitted in clear text across transmission media are susceptible to eavesdropping by adversaries, who could reuse them to gain unauthorized access to a network device. Such access could allow an adversary to disrupt ICS operations or to monitor ICS network activity.
Passwords exist indefinitely on network devices	Passwords should be changed regularly so that if one becomes known by an unauthorized party, the party has unauthorized access to the network device only for a short time. Such access could allow an adversary to disrupt ICS operations or monitor ICS network activity.
Inadequate access controls applied	Unauthorized access to network devices and administrative functions could allow a user to disrupt ICS operations or monitor ICS network activity.

Table 3-9. Network Hardware Vulnerabilities

Vulnerability	Description
Inadequate physical protection of network equipment	Access to network equipment should be controlled to prevent damage or destruction.
Unsecured physical ports	Unsecured universal serial bus (USB) and PS/2 ports could allow unauthorized connection of thumb drives, keystroke loggers, etc.
Loss of environmental control	Loss of environmental control could lead to processors overheating. Some processors will shut down to protect themselves, and some just melt if they overheat.
Non-critical personnel have access to equipment and network connections	Physical access to network equipment should be restricted to only the necessary personnel. Improper access to network equipment can lead to any of the following: • Physical theft of data and hardware • Physical damage or destruction of data and hardware • Unauthorized changes to the security environment (e.g., altering ACLs to permit attacks to enter a network) • Unauthorized interception and manipulation of network activity • Disconnection of physical data links or connection of unauthorized data links
Lack of redundancy for critical networks	Lack of redundancy in critical networks could provide single point of failure possibilities

Table 3-10. Network Perimeter Vulnerabilities

Vulnerability	Description
No security perimeter defined	If the control network does not have a security perimeter clearly defined, then it is not possible to ensure that the necessary security controls are deployed and configured properly. This can lead to unauthorized access to systems and data, as well as other problems.
Firewalls nonexistent or improperly configured	A lack of properly configured firewalls could permit unnecessary data to pass between networks, such as control and corporate networks. This could cause several problems, including allowing attacks and malware to spread between networks, making sensitive data susceptible to monitoring/eavesdropping on the other network, and providing individuals with unauthorized access to systems.
Control networks used for non-control traffic	Control and non-control traffic have different requirements, such as determinism and reliability, so having both types of traffic on a single network makes it more difficult to configure the network so that it meets the requirements of the control traffic. For example, non-control traffic could inadvertently consume resources that control traffic needs, causing disruptions in ICS functions.
Control network services not within the control network	Where IT services such as Domain Name System (DNS),and/or Dynamic Host Configuration Protocol (DHCP) are used by control networks, they are often implemented in the IT network, causing the ICS network to become dependent on the IT network that may not have the reliability and availability requirements needed by the ICS.

Table 3-11. Network Monitoring and Logging Vulnerabilities

Vulnerability	Description
Inadequate firewall and router logs	Without proper and accurate logs, it might be impossible to determine what caused a security incident to occur.
No security monitoring on the ICS network	Without regular security monitoring, incidents might go unnoticed, leading to additional damage and/or disruption. Regular security monitoring is also needed to identify problems with security controls, such as misconfigurations and failures.

Table 3-12. Communication Vulnerabilities

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

Table 3-13. Wireless Connection Vulnerabilities

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

3.4 Risk Factors

Several factors currently contribute to the increasing risk to control systems, which are discussed in greater detail in Sections 3.4.1 through 3.4.4:

- Adoption of standardized protocols and technologies with known vulnerabilities
- Connectivity of the control systems to other networks
- Insecure and rogue connections
- Widespread availability of technical information about control systems.

3.4.1 Standardized Protocols and Technologies

ICS vendors have begun to open up their proprietary protocols and publish their protocol specifications to enable third-party manufacturers to build compatible accessories. Organizations are also transitioning from proprietary systems to less expensive, standardized technologies such as Microsoft Windows and Unix-like operating systems as well as common networking protocols such as TCP/IP to reduce costs and improve performance. Another standard contributing to this evolution of open systems is OPC, a protocol that enables interaction between control systems and PC-based application programs. The transition to using these open protocol standards provides economic and technical benefits, but also increases the susceptibility of ICS to cyber incidents. These standardized protocols and technologies have commonly known vulnerabilities, which are susceptible to sophisticated and effective exploitation tools that are widely available and relatively easy to use.

3.4.2 Increased Connectivity

ICS and corporate IT systems are often interconnected as a result of several changes in information management practices, operational, and business needs. The demand for remote access has encouraged many organizations to establish connections to the ICS that enable ICS engineers and support personnel to monitor and control the system from points outside the control network. Many organizations have also added connections between corporate networks and ICS networks to allow the organization's decision makers to obtain access to critical data about the status of their operational systems and to send instructions for the manufacture or distribution of product. In early implementations this might have been done with custom applications software or via an OPC server/gateway; however, in the past ten years this has been accomplished with Transmission Control Protocol/Internet Protocol (TCP/IP) networking and standardized IP applications like File Transfer Protocol (FTP) or Extensible Markup Language (XML) data exchanges. Often, these connections were implemented without a full understanding of the corresponding security risks. In addition, corporate networks are often connected to strategic partner networks and to the Internet. Control systems also make more use of WANs and the Internet to transmit data to their remote or local stations and individual devices. This integration of control system networks with public and corporate networks increases the accessibility of control system vulnerabilities. Unless appropriate security controls are deployed, these vulnerabilities can expose all levels of the ICS network architecture to complexity-induced error, adversaries and a variety of cyber threats, including worms and other malware. As an example of the change in threats to control systems, an internal survey of an unnamed energy organization showed the following:

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

Adding to the complexity of the situation, the goals of IT departments can be fundamentally different from those of process control departments. The IT world typically sees performance, confidentiality, and data integrity as paramount, while the ICS world sees human and plant safety as its primary responsibility, and thus system availability and data integrity are core priorities. Other distinctions, as discussed in Section 3.1, include differences in reliability requirements, incident impacts, performance expectations, operating systems, communications protocols, and system architectures. This can mean significant differences in implementation of security practices.

3.4.3 Insecure and Rogue Connections

Many ICS vendors have delivered systems with dial-up modems that provide remote access to ease the burdens of maintenance for the technical field support personnel. Remote access sometimes provides support staff with administrative-level access to a system, such as using a telephone number, and sometimes an access control credential (e.g., valid ID, and/or a password). Adversaries with *war dialers*—simple personal computer programs that dial consecutive phone numbers looking for modems—and password cracking software could gain access to systems through these remote access capabilities. Passwords used for remote access are often common to all implementations of a particular vendor's systems and may have not been changed by the end user. These types of connections can leave a system highly vulnerable because people entering systems through vendor-installed modems are often granted high levels of system access.

Organizations often inadvertently leave access links such as dial-up modems open for remote diagnostics, maintenance, and monitoring. Also, control systems increasingly utilize wireless communications systems, which can be vulnerable. Access links not protected with authentication and/or encryption have the increased risk of adversaries using these unsecured connections to access remotely controlled systems. This could lead to an adversary compromising the integrity of the data in transit as well as the availability of the system, both of which can result in an impact to public and plant safety. Before deploying encryption, first determine if encryption is an appropriate solution for the specific ICS application. Section 6.3.4.1 provides additional information on the use of encryption in the ICS environment.

Many of the interconnections between corporate networks and ICS require the integration of systems with different communications standards. The result is often an infrastructure that is engineered to move data successfully between two unique systems. Because of the complexity of integrating disparate systems, control engineers often fail to address the added burden of accounting for security risks. Many control engineers have little if any training in security and often IT security personnel are not involved in ICS security design. As a result, access controls designed to protect control systems from unauthorized access through corporate networks are usually minimal. Moreover, the behavior of the underlying protocols may not be well understood, and thus vulnerabilities can exist that can defeat even advanced security countermeasures. Protocols, such as TCP/IP and others have characteristics that often go unchecked, and this may counter any security that can be done at the network or the application levels.

3.4.4 Public Information

Public information regarding ICS design, maintenance, interconnection, and communication is readily available over the Internet to support competition in product choices as well as to enable the use of open standards. ICS vendors also sell toolkits to help develop software that implements the various standards used in ICS environments. There are also many former employees, vendors, contractors, and other end users of the same ICS equipment worldwide who have inside knowledge about the operation of control systems and processes. For example, one person used his inside knowledge of a system to cause one of the most cited ICS cyber security incidents, the Maroochy Shire sewage spill. Additional information on the Maroochy Shire sewage spill incident is available in Section 3.7.

Information and resources are available to potential adversaries and intruders of all calibers around the world. With the available information, it is quite possible for an individual with very little knowledge of control systems to gain unauthorized access to a control system with the use of automated attack and data mining tools and a factory-set default password. Many times, these default passwords are never changed.

3.5 Possible Incident Scenarios

There are many possible incident scenarios for an ICS including [10]:

- Control systems operation disrupted by delaying or blocking the flow of information through corporate or control networks, thereby denying availability of the networks to control system operators or causing information transfer bottlenecks or denial of service by IT-resident services (such as DNS)
- Unauthorized changes made to programmed instructions in PLCs, RTUs, DCS, or SCADA controllers, alarm thresholds changed, or unauthorized commands issued to control equipment, which could potentially result in damage to equipment (if tolerances are exceeded), premature shutdown of processes (such as prematurely shutting down transmission lines), causing an environmental incident, or even disabling control equipment
- False information sent to control system operators either to disguise unauthorized changes or to initiate inappropriate actions by system operators
- Control system software or configuration settings modified, producing unpredictable results
- Safety systems operation interfered with
- Malicious software (e.g., virus, worm, Trojan horse) introduced into the system
- Recipes (i.e., the materials and directions for creating a product) or work instructions modified in order to bring about damage to products, equipment, or personnel

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

The following are two hypothetical ICS incident scenarios [11]:

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

Although these scenarios are hypothetical, they represent potential incident scenarios for an ICS. Section 3.7 provides summaries of several actual ICS incidents.

3.6 Sources of Incidents

An accurate accounting of cyber incidents on control systems is difficult to determine. However, individuals in the industry who have been focusing on this issue see similar growth trends between vulnerabilities exposed in traditional IT systems and those being found in control systems. There is a Repository of Security Incidents (RISI)[3], which is designed to track incidents of a cyber security nature that directly affect ICS and processes. This includes events such as accidental cyber-related incidents, as well as deliberate events such as unauthorized remote access, DoS attacks, and malware infiltrations. Data is collected through research into publicly known incidents and from private reporting by member organizations that wish to have access to the database. Each incident is investigated and then rated according to reliability (confirmed, likely but unconfirmed, unlikely or unknown, and hoax/urban legend).

The data collected includes the following:

- Incident title
- Date of incident
- Reliability of report
- Type of incident (e.g., accident, virus)
- Industry (e.g., petroleum, automotive)
- Entry point (e.g., Internet, wireless, modem)
- Perpetrator
- Type of system and hardware impacted
- Brief description of incident
- Impact on organization
- Measures to prevent recurrence
- References.

As of June 2006, 119 incidents had been investigated and logged in the database, with 15 incidents still pending investigation. Of these, 13 were flagged as hoax or unlikely and removed from the study data. Figure 3-1 shows the trend of incidents between 1982 and 2006, which shows a sharp increase in incidents starting around 2001. The complexity of modern ICS leaves many vulnerabilities as well as vectors for attack. Attacks can come from many places, including indirectly through the corporate network or directly via the Internet, virtual private networks (VPN), wireless networks, and dial-up modems.

[3] The Repository of Security Incidents (RISI) can be found at: http://www.securityincidents.org/