SCADA 202

CONTINUING EDUCATION
PROFESSIONAL DEVELOPMENT COURSE

Technical Learning College

Printing and Saving Instructions

TLC recommends that you download and save this pdf document and assignment to your computer desktop and open it with Adobe Acrobat DC reader.

Adobe Acrobat DC reader is a free computer software program and you can find it at Adobe Acrobat's website.

You can complete the course by viewing the course on your computer or you can print it out. This course booklet does not have the assignment (the test). Please visit our website and download the assignment (the test).

Printing Instructions: Once you have purchased the program, we will give you permission to print this document. If you are going to print this document, it was designed to be printed double-sided or duplexed but can be printed single-sided.

Hyperlink to Assignment…
http://www.abctlc.com/downloads/PDF/SCADA202Ass.pdf

State Approval Listing Link, check to see if your State accepts or has pre-approved this course. Not all States are listed. Not all courses are listed. Do not solely trust our list for it may be outdated. It is your sole responsibility to ensure this course is accepted for credit. No refunds.

Professional Engineers; Most states will accept our courses for credit but we do not officially list the States or Agencies acceptance or approvals.

State Approval Listing URL…
http://www.abctlc/PDF/CEU%20State%20Approvals.pdf

You can obtain a printed version from TLC for an additional $129.95 plus shipping charges.

All downloads are electronically tracked and monitored for security purposes.

Safety Always

1. Be Safety Conscious
Working with electrical circuits can be dangerous if you do not take certain safety precautions. Electrical shock can not only injure you but also kill you. Practice safety when working on any circuit and slow down! When you hurry through a project, there is a greater chance for an accident to occur.

2. Shut the Power Off
Always shut off the power to a circuit or device that you will be working on. This is the first thing you should do before working on any electrical circuit. I do not know anyone who has been shocked by a circuit that is not energized.

3. Test the Circuit
After turning a circuit off, it is a good idea to check it with a tester to be sure that, indeed, it is off. Never assume that the circuit is off!

4. Ladders
Ladders are necessary to accomplish some electrical jobs. Never use an aluminum ladder on any electrical project. Always use an insulated fiberglass ladder to keep you safe.

5. Wet Locations
Avoid wet areas when working with or on anything electrical. If there is a reason that you have to be in that situation, wear rubber boots and gloves to lesson your chance of getting shocked. Tools and appliances should be plugged into a GFCI outlet or GFCI extension cord.

Do not forget to dry your hands before grabbing any cord to plug it in or unplug it. Wet hands and a frayed cord do not mix. You reach down to grab the cord and just like that, you have been shocked! Believe it or not, it happens.

6. Warning Labels
Finally, if you are working on the service panel or a circuit, be sure to place a warning label on the face of the panel. This will warn someone not to turn on the circuit that you are working on. There is nothing worse than turning off the power, checking that it is off and starting to work on the circuit, only to have someone come behind you and turn the circuit back on. Always think and ask questions before turning on a breaker that is shut off. Maybe someone is working on the other end.

Some States and many employers require the final exam to be proctored.

Do not solely depend on TLC's Approval list for it may be outdated.

Most of our students prefer to do the assignment in Word and e-mail or fax the assignment back to us. We also teach this course in a conventional hands-on class. Call us and schedule a class today.

Important Information about this Manual

Disclaimer

This CEU training manual has been prepared to assist employees in the general awareness of the dangerous SCADA and /or electrical system, dealing with often-complex procedures and requirements for safely handling hazardous energy. The scope of the material is quite large, requiring a major effort to bring it under control. Employee health and safety, as well as that of the public, depend upon careful application of federal and state regulations and safe working procedures.

This course will cover general electrical laws, and work rules relating to electrical principles. It should be noted, however, that the federal and state regulations are an ongoing process and subject to change over time. This manual is a guidance document for employees who are learning general SCADA and/or electrical principles.

This course is not designed to meet the full requirements of the United States Environmental Protection Agency (EPA) or the Department of Labor-Occupational Safety and Health Administration (OSHA) rules and regulations. Only qualified licensed electricians should be allowed to work on any or all electrical installations or components. This course will not qualify you to work on any type of electrical system or component.

This course manual will provide general guidance and should not be used as a preliminary basis for developing any type of electrical or safety plan or procedure. This document is not detailed electrical procedure or electrical safety textbook or a comprehensive source book on electrical safety or building codes rules and regulations.

Technical Learning College makes no warranty, guarantee or representation as to the absolute correctness or appropriateness of the information in this manual and assumes no responsibility in connection with the implementation of this information.

It cannot be assumed that this manual contains all measures and concepts required for specific conditions or circumstances. This document should be used for guidance and is not considered a legal document.

Individuals who are responsible for electrical repairs or installation and the health and safety of workers should obtain and comply with the most recent federal, state, and local regulations relevant to these sites and are urged to consult with OSHA, the EPA and other appropriate federal, state, and local agencies.

Copyright Notice

Contributing Editors

James L. Six Received a Bachelor of Science Degree in Civil Engineering from the University of Akron in June of 1976, Registered Professional Engineer in the State of Ohio, Number 45031 (Retired), Class IV Water Supply Operator issued by Ohio EPA, Number WS4-1012914-08, Class II Wastewater Collection System Operator issued by Ohio EPA, Number WC2-1012914-94

Joseph Camerata has a BS in Management with honors (magna cum laude). He retired as a Chemist in 2006 having worked in the field of chemical, environmental, and industrial hygiene sampling and analysis for 40 years.

James Bevan, Water Quality Inspector S.M.E. Twenty years of experience in the environmental field dealing with all aspects of water regulations on the federal, state, and local levels. Teacher and Proctor in Charge for Backflow Certification Testing at the ASETT Center in Tucson for the past 15 years and possess an Arizona Community College, Special Teaching Certificate in Environmental Studies.

Dr. Pete Greer S.M.E., Retired biology instructor, chemistry and biological review.

Jack White, Environmental, Health, Safety expert, City of Phoenix. Art Credits.

Course Credits

Most of the course text will come from *National Institute of Standards and Technology Special Publication 800-82 (INITIAL PUBLIC DRAFT) Natl. Inst. Stand. Technol. Spec. Publ. 800-82, 164 pages (September 2006)*

Acknowledgments

The authors, Keith Stouffer, Joe Falco, and Karen Kent of the National Institute of Standards and Technology (NIST), wish to thank their colleagues who reviewed drafts of this document and contributed to its technical content. The authors would particularly like to acknowledge Tim Grance, Ron Ross and Stu Katzke of NIST for their keen and insightful assistance throughout the development of the document. The authors also gratefully acknowledge and appreciate the many contributions from the public and private sectors whose thoughtful and constructive comments improved the quality and usefulness of this publication. The authors would particularly like to thank the members of the Process Control Security Requirements Forum (PCSRF) and ISA-SP99. The authors would also like to thank the UK National Infrastructure Security Coordination Centre (NISCC) for allowing portions of the NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Network to be used in this document as well as ISA for allowing portions of TR99.00.01: Security Technologies for Manufacturing and Control System and TR99.00.02: Integrating Electronic Security into the Manufacturing and Control Systems Environment to be used in this document.

Technical Learning College's Scope and Function

Welcome to the Program,

Technical Learning College (TLC) offers affordable continuing education for today's working professionals who need to maintain licenses or certifications. TLC holds several different governmental agency approvals for granting of continuing education credit.

TLC's delivery method of continuing education can include traditional types of classroom lectures and distance-based courses or independent study. TLC's distance based or independent study courses are offered in a print - based distance educational format. We will beat any other training competitor's price for the same CEU material or classroom training.

Our courses are designed to be flexible and for you to finish the material at your convenience. Students can also receive course materials through the mail. The CEU course or e-manual will contain all your lessons, activities and instruction to obtain the assignments. All of TLC's CEU courses allow students to submit assignments using e-mail or fax, or by postal mail. (See the course description for more information.)

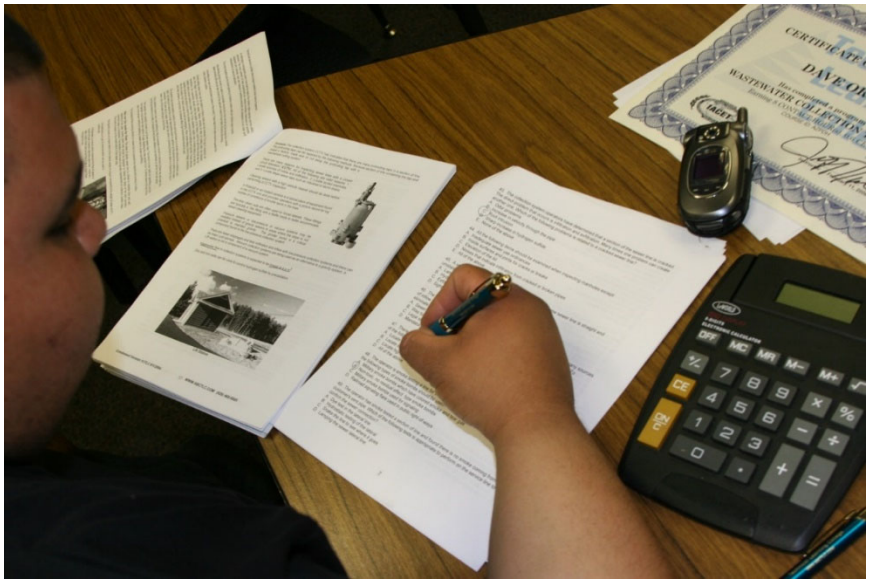
Students have direct contact with their instructor—primarily by e-mail or telephone. TLC's CEU courses may use such technologies as the World Wide Web, e-mail, CD-ROMs, videotapes and hard copies. (See the course description.) Make sure you have access to the necessary equipment before enrolling; i.e., printer, Microsoft Word and/or Adobe Acrobat Reader. Some courses may require proctored closed-book exams, depending upon your state or employer requirements.

Flexible Learning
At TLC there are no scheduled online sessions or passwords you need contend with, nor are you required to participate in learning teams or groups designed for the "typical" younger campus based student. You will work at your own pace, completing assignments in time frames that work best for you. TLC's method of flexible individualized instruction is designed to provide each student the guidance and support needed for successful course completion.

Course Structure
TLC's online courses combine the best of online delivery and traditional university textbooks. You can easily find the course syllabus, course content, assignments, and the post-exam (Assignment). This student-friendly course design allows you the most flexibility in choosing when and where you will study.

Classroom of One
TLC offers you the best of both worlds. You learn on your own terms, on your own time, but you are never on your own. Once enrolled, you will be assigned a personal Student Service Representative who works with you on an individualized basis throughout your program of study. Course specific faculty members (S.M.E.) are assigned at the beginning of each course providing the academic support you need to successfully complete each course. Please call or email us for assistance.

Satisfaction Guaranteed
We have many years of experience, dealing with thousands of students. We assure you, our customer satisfaction is second to none. This is one reason we have taught more than 20,000 students.



We welcome you to do the electronic version of the assignment and submit the answer key and registration to us either by fax or e-mail. If you need this assignment graded and a certificate of completion within a 48-hour turn around, prepare to pay an additional rush charge of $50.

Contact Numbers

Fax (928) 468-0675
Email Info@tlch2o.com
Telephone (866) 557-1746

TLC's CEU Course Description

SCADA 202 CEU TRAINING COURSE

This CEU course is a review of various industrial controls i.e. SCADA, telemetry and security principles. This course is general in nature and not state specific. You will not need any other materials for this course.

- How to monitor water/wastewater equipment.
- How to adjust various water/wastewater equipment.
- How to protect SCADA systems and related assets.

You will not need any other materials for this course.

Target Audience

The primary target audience for this course includes SCADA operators, electricians, instrument technicians or maintenance technicians but is not limited to include water distribution workers, well drillers, pump installers, water treatment operators, wastewater operators and onsite/installers.

Also included are people interested in working in a water treatment/wastewater treatment or distribution facility and/or wishing to maintain CEUs for a certification license or to learn how to perform their job safely and effectively, and/or to meet education needs for promotion. There are no prerequisites, and no other materials are needed for this course.

Course Procedures for Registration and Support

All of Technical Learning College's correspondence courses have complete registration and support services offered. Delivery of services will include, e-mail, web site, telephone, fax and mail support. TLC will attempt immediate and prompt service.

When a student registers for a distance or correspondence course, he/she is assigned a start date and an end date. It is the student's responsibility to note dates for assignments and keep up with the course work. If a student falls behind, he/she must contact TLC and request an end date extension in order to complete the course. It is the prerogative of TLC to decide whether to grant the request. All students will be tracked by a unique number assigned to the student.

Instructions for Written Assignments

The SCADA 202 CEU Training course uses a multiple choice answer key. If you should need any assistance, please email all concerns and the final test to: info@tlch2o.com.

You may write your answers or type out your own answer key. TLC would prefer that you utilize the answer key found on the TLC website under Assignments and e-mail the answer key to TLC, but it is not required. You may also fax the answer key. Please call us a couple hours later to ensure we received your information.

Feedback Mechanism (Examination Procedures)

Each student will receive a feedback form as part of their study packet. You will be able to find this form in the front of the course assignment or lesson.

Security and Integrity

All students are required to do their own work. All lesson sheets and final exams are not returned to the student to discourage sharing of answers. Any fraud or deceit and the student will forfeit all fees and the appropriate agency will be notified.

Grading Criteria
TLC will offer the student either pass/fail or a standard letter grading assignment. If TLC is not notified, you will only receive a pass/fail notice.

Required Texts
The SCADA 202 CEU Training course will not require any other materials. This course comes complete. No other materials are needed.

Recordkeeping and Reporting Practices
TLC will keep all student records for a minimum of seven years. It is the student's responsibility to give the completion certificate to the appropriate agencies.

ADA Compliance
TLC will make reasonable accommodations for persons with documented disabilities.

Students should notify TLC and their instructors of any special needs. Course content may vary from this outline to meet the needs of this particular group.

You will have 90 days from receipt of this manual to complete it in order to receive your Continuing Education Units (CEUs) or Professional Development Hours (PDHs). A score of 70% or better is necessary to pass this course.

Educational Mission

The educational mission of TLC is:
To provide TLC students with comprehensive and ongoing training in the theory and skills needed for the environmental education field,

To provide TLC students with opportunities to apply and understand the theory and skills needed for operator certification,

To provide opportunities for TLC students to learn and practice environmental educational skills with members of the community for the purpose of sharing diverse perspectives and experience,

To provide a forum in which students can exchange experiences and ideas related to environmental education,

To provide a forum for the collection and dissemination of current information related to environmental education, and to maintain an environment that nurtures academic and personal growth.

Table of Contents

SCADA Acronyms and Abbreviations

Selected acronyms and abbreviations used in the *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security* are defined below.

AC Access Control
AC Alternating Current
ACL Access Control List
AGA American Gas Association
API American Petroleum Institute
ARP Address Resolution Protocol
BCP Business Continuity Plan
CC Common Criteria
CD Compact Disc
CHAP Challenge Handshake Authentication Protocol
CIDX Chemical Industry Data Exchange
CIGRE International Council on Large Electric Systems
CIP Critical Infrastructure Protection
CIPC Critical Infrastructure Protection Committee
CMVP Cryptographic Module Validation Program
COTS Commercial Off-the-Shelf
CPU Central Processing Unit
CSE Communications Security Establishment
CSRC Computer Security Resource Center
CSSC Control System Security Center
CVE Common Vulnerabilities and Exposures
DCOM Distributed Component Object Model
DCS Distributed Control System
DETL Distributed Energy Technology Laboratory
DHS Department of Homeland Security
DMZ Demilitarized Zone
DNP Distributed Network Protocol
DNS Domain Name System
DOE Department of Energy
DoS Denial of Service
DRP Disaster Recovery Plan
DVD Digital Video Disc
EAP Extensible Authentication Protocol
EMS Energy Management System
EPRI Electric Power Research Institute
ERP Enterprise Resource Planning
FIPS Federal Information Processing Standards
FISMA Federal Information Security Management Act
FTP File Transfer Protocol

GAO Government Accountability Office
GPS Global Positioning System
HMI Human-Machine Interface
HSARPA Homeland Security Advanced Research Projects Agency
HSPD Homeland Security Presidential Directive
HTTP Hypertext Transfer Protocol
HTTPS Hypertext Transfer Protocol Secure
HVAC Heating, Ventilation, and Air Conditioning
I/O Input/Output
I3P Institute for Information Infrastructure Protection
IAONA Industrial Automation Open Networking Association
ICS Industrial Control System
IDS Intrusion Detection System
IEC International Electrotechnical Commission
IED Intelligent Electronic Device
IEEE Institute of Electrical and Electronics Engineers
IETF Internet Engineering Task Force
IGMP Internet Group Management Protocol
INL Idaho National Laboratory
IO Input/Output
IP Internet Protocol
IPS Intrusion Prevention System
IPsec Internet Protocol Security
ISA ISA-The Instrumentation Systems and Automation Society
ISAC Information Sharing and Analysis Center
ISID Industrial Security Incident Database
ISO International Standards Organization
IT Information Technology
ITL Information Technology Laboratory
LAN Local Area Network
MAC Media Access Control
MES Manufacturing Execution System
MIB Management Information Base
MTU Master Terminal Unit (also Master Telemetry Unit)
NAT Network Address Translation
NCSD National Cyber Security Division
NERC North American Electric Reliability Council
NFS Network File System
NIAP National Information Assurance Partnership
NIC Network Interface Card
NISAC National Infrastructure Simulation and Analysis Center
NISCC National Infrastructure Security Coordination Centre
NIST National Institute of Standards and Technology
NSTB National SCADA Testbed

OEA Office of Energy Assurance
OEM Original Equipment Manufacturers
OLE Object Linking and Embedding
OMB Office of Management and Budget
OPC OLE for Process Control
OS Operating System
OSI Open Systems Interconnection
PCN Process Control Network
PCSF Process Control System Forum
PCSRF Process Control Security Requirements Forum
PDA Personal Digital Assistant
PEAP Protected Extensible Authentication Protocol
PIN Personal Identification Number
PID Proportional – Integral - Derivative
PIV Personal Identity Verification
PLC Programmable Logic Controller
PP Protection Profile
PPP Point-to-Point Protocol
R&D Research and Development
RADIUS Remote Authentication Dial In User Service
RBAC Role-Based Access Control
RF Radio Frequency
RFC Request for Comments
RMA Reliability, Maintainability, and Availability
RPC Remote Procedure Call
RPO Recovery Point Objective
RTO Recovery Time Objective
RTU Remote Terminal Unit (also Remote Telemetry Unit)
SC Security Category
SCADA Supervisory Control and Data Acquisition
SCP Secure Copy
SIS Safety Instrumented System
SMTP Simple Mail Transfer Protocol
SNL Sandia National Laboratories
SNMP Simple Network Management Protocol
SP Special Publication
SPP-ICS System Protection Profile for Industrial Control Systems
SQL Structured Query Language
SRP Salt River Project
SSH Secure Shell
SSID Service Set Identifier
SSL Secure Sockets Layer
TCP Transmission Control Protocol
TCP/IP Transmission Control Protocol/Internet Protocol
TFTP Trivial File Transfer Protocol
TLS Transport Layer Security

UDP User Datagram Protocol
UPS Uninterruptible Power Supply
US-CERT United States Computer Emergency Readiness Team
USB Universal Serial Bus
USSR Union of Soviet Socialist Republics
VFD Variable Frequency Drive
VLAN Virtual Local Area Network
VPN Virtual Private Network
WAN Wide Area Network
XML Extensible Markup Language

Key Terms

Communication Infrastructure
This connects the supervisory computer system to the RTUs and PLCs, and may use industry standard or manufacturer proprietary protocols. Both RTU's and PLC's operate autonomously on the near-real time control of the process, using the last command given from the supervisory system. Failure of the communications network does not necessarily stop the plant process controls, and on resumption of communications, the operator can continue with monitoring and control. Some critical systems will have dual redundant data highways, often cabled via diverse routes.

HMI - Human-Machine Interface
The human-machine interface (HMI) is the operator window of the supervisory system. It presents plant information to the operating personnel graphically in the form of mimic diagrams, which are a schematic representation of the plant being controlled, and alarm and event logging pages. The HMI is linked to the SCADA supervisory computer to provide live data to drive the mimic diagrams, alarm displays and trending graphs. In many installations the HMI is the graphical user interface for the operator, collects all data from external devices, creates reports, performs alarming, sends notifications, etc.

Mimic diagrams consist of line graphics and schematic symbols to represent process elements, or may consist of digital photographs of the process equipment overlain with animated symbols. Supervisory operation of the plant is by means of the HMI, with operators issuing commands using mouse pointers, keyboards and touch screens.

For example, a symbol of a pump can show the operator that the pump is running, and a flow meter symbol can show how much fluid it is pumping through the pipe. The operator can switch the pump off from the mimic by a mouse click or screen touch. The HMI will show the flow rate of the fluid in the pipe decrease in real time.

The HMI package for a SCADA system typically includes a drawing program that the operators or system maintenance personnel use to change the way these points are represented in the interface. These representations can be as simple as an on-screen traffic light, which represents the state of an actual traffic light in the field, or as complex as a multi-projector display representing the position of all of the elevators in a skyscraper or all of the trains on a railway.

A "historian", is a software service within the HMI which accumulates time-stamped data, events, and alarms in a database which can be queried or used to populate graphic trends in the HMI. The historian is a client that requests data from a data acquisition server.

PLCs - Programmable Logic Controllers
Also known as PLCs, these are connected to sensors and actuators in the process, and are networked to the supervisory system in the same way as RTUs. PLCs have more sophisticated embedded control capabilities than RTUs, and are programmed in one or more IEC 61131-3 programming languages. PLCs are often used in place of RTUs as field devices because they are more economical, versatile, flexible and configurable.

RTU- Remote Terminal Units
Remote terminal units, also known as (RTUs), connect to sensors and actuators in the process, and are networked to the supervisory computer system. RTUs are "intelligent I/O" and often have embedded control capabilities such as ladder logic in order to accomplish Boolean logic operations.

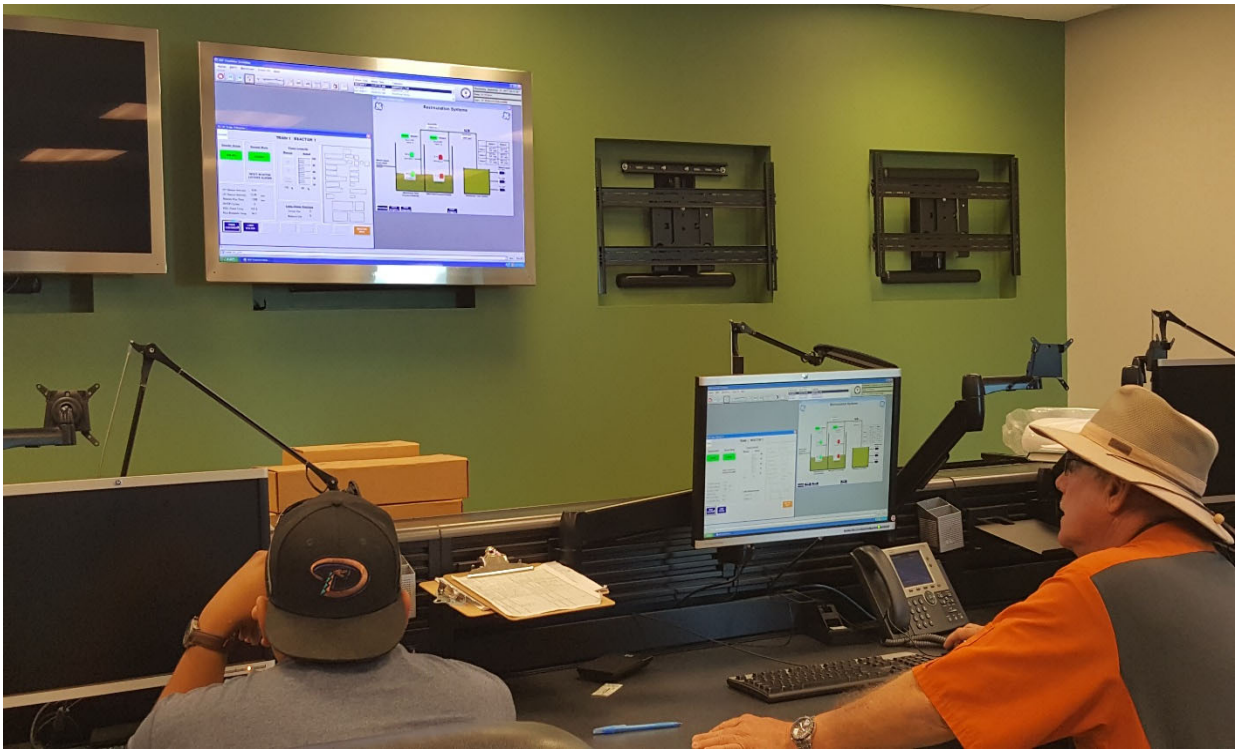
SCADA – Supervisory Control and Data Acquisition
SCADA is an acronym for supervisory control and data acquisition, a computer system for gathering and analyzing real time data. SCADA systems are used to monitor and control a plant or equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining and transportation.

Supervisory Computers
This is the core of the SCADA system, gathering data on the process and sending control commands to the field connected devices. It refers to the computer and software responsible for communicating with the field connection controllers, which are RTUs and PLCs, and includes the HMI software running on operator workstations.

In smaller SCADA systems, the supervisory computer may be composed of a single PC, in which case the HMI is a part of this computer. In larger SCADA systems, the master station may include several HMIs hosted on client computers, multiple servers for data acquisition, distributed software applications, and disaster recovery sites. To increase the integrity of the system the multiple servers will often be configured in a dual-redundant or hot-standby formation providing continuous control and monitoring in the event of a server malfunction or breakdown.

Topic 1 – SCADA Introduction

Topic 1 - Section Focus: You will learn the basics of the SCADA (or supervisory control and data acquisition) system. You will be able to understand and describe the purpose of SCADA and the basic operation of SCADA systems. There is a post quiz at the end of this section to review your comprehension and a final examination in the Assignment for your contact hours.
Topic 1 – Scope/Background: Industrial organizations and companies in the public and private sectors to control and maintain efficiency, distribute data for smarter decisions, and communicate system issues to help mitigate downtime use SCADA systems.



What is SCADA and Who Uses It?

Supervisory control and data acquisition (SCADA) is a system of software and hardware elements that allows industrial organizations to:

- Control industrial processes locally or at remote locations
- Monitor, gather, and process real-time data
- Directly interact with devices such as sensors, valves, pumps, motors, and more through human-machine interface (HMI) software
- Record events into a log file

SCADA systems are crucial for industrial organizations since they help to maintain efficiency, process data for smarter decisions, and communicate system issues to help mitigate downtime.

The basic SCADA architecture begins with programmable logic controllers (PLCs) or remote terminal units (RTUs). PLCs and RTUs are microcomputers that communicate with an array of objects such as factory machines, HMIs, sensors, and end devices, and then route the information from those objects to computers with SCADA software. The SCADA software processes, distributes, and displays the data, helping operators and other employees analyze the data and make important decisions.

For example, the SCADA system quickly notifies an operator that a batch of product is showing a high incidence of errors. The operator pauses the operation and views the SCADA system data via an HMI to determine the cause of the issue. The operator reviews the data and discovers that Machine 4 was malfunctioning. The SCADA system's ability to notify the operator of an issue helps him to resolve it and prevent further loss of product.

SCADA systems are used by industrial organizations and companies in the public and private sectors to control and maintain efficiency, distribute data for smarter decisions, and communicate system issues to help mitigate downtime.

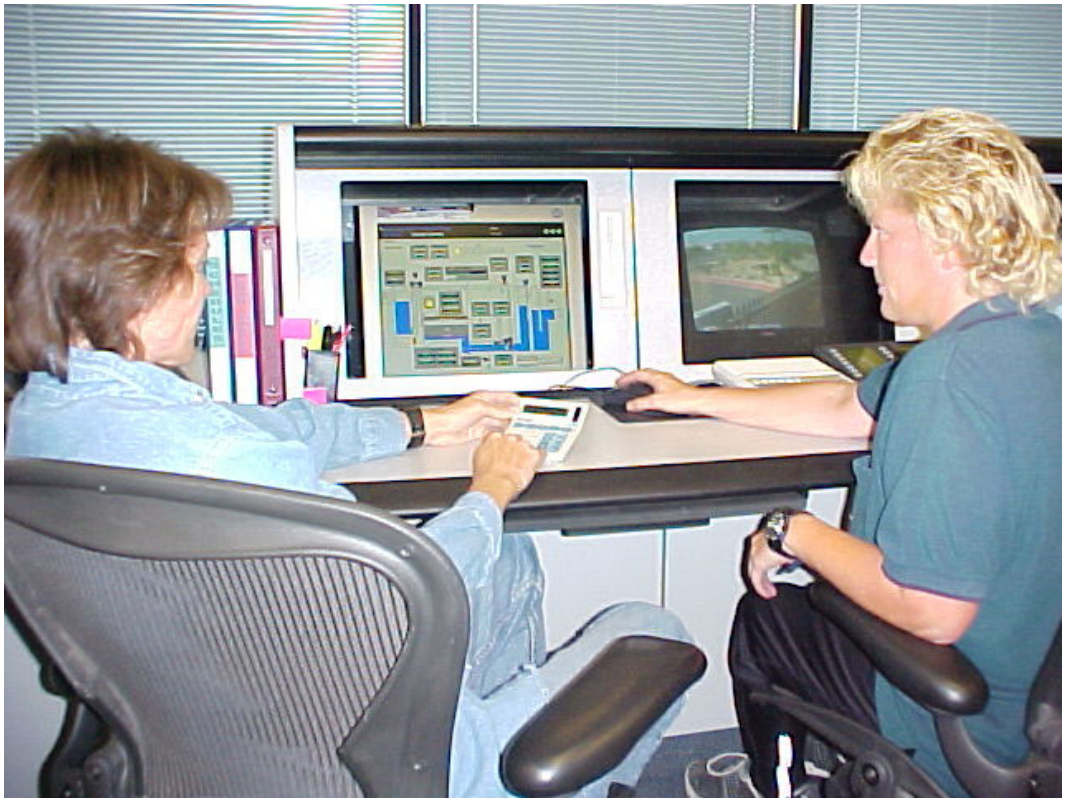
SCADA systems work well in many different types of enterprises because they can range from simple configurations to large, complex installations. SCADA systems are the backbone of many modern industries, including:

- Energy
- Food and beverage
- Manufacturing
- Oil and gas
- Power
- Recycling
- Transportation
- Water and wastewater
- And many more

Virtually anywhere you look in today's world, there is some type of SCADA system running behind the scenes: maintaining the refrigeration systems at the local supermarket, ensuring production and safety at a refinery, achieving quality standards at a waste water treatment plant, or even tracking your energy use at home, to give a few examples.

Effective SCADA systems can result in significant savings of time and money. Numerous case studies have been published highlighting the benefits and savings of using a modern SCADA software solution such as Ignition.

SCADA Explained



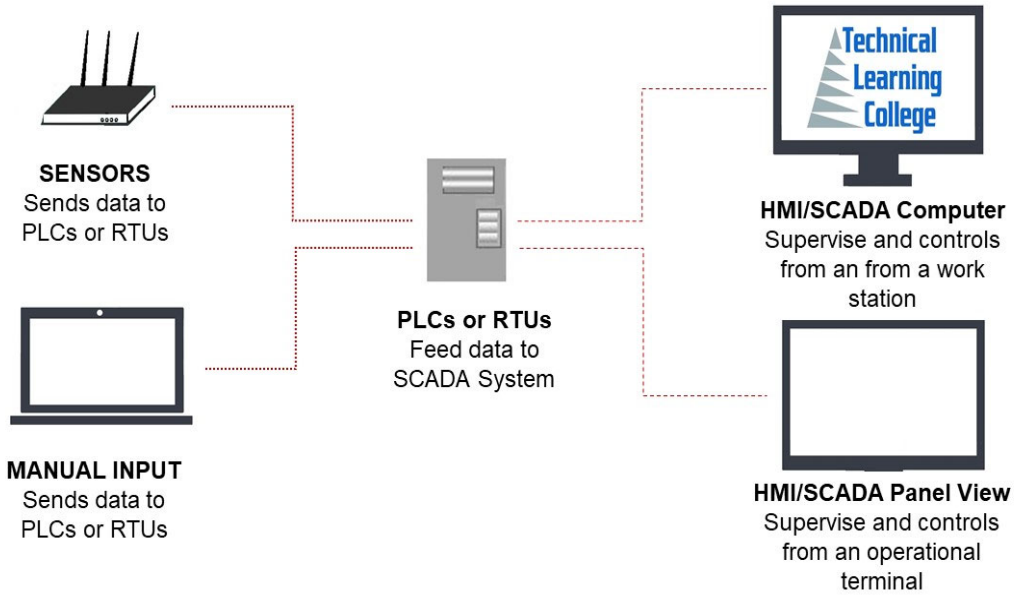
Supervisory control and data acquisition – SCADA refers to ICS (industrial control systems) used to control infrastructure processes (water treatment, wastewater treatment, gas pipelines, wind farms, etc.), facility-based processes (airports, space stations, ships, etc.,) or industrial processes (production, manufacturing, refining, power generation, etc.).

Supervisory Control and Data Acquisition (SCADA) is a control system architecture that uses computers, networked data communications and graphical user interfaces for high-level process supervisory management, but uses other peripheral devices such as programmable logic controller (PLC) and discrete PID controllers to interface with the process plant or machinery. The use of SCADA has been also considered for management and operations of project-driven-process in construction.

The following subsystems are usually present in SCADA systems:

- The apparatus used by a human operator; all the processed data are presented to the operator
- A supervisory system that gathers all the required data about the process
- Remote Terminal Units (RTUs) connected to the sensors of the process, which helps to convert the sensor signals to the digital data and send the data to supervisory stream.
- Programmable Logic Controller (PLCs) used as field devices
- Communication infrastructure connects the Remote Terminal Units to supervisory system.

Generally, a SCADA system does not control the processes in real time – it usually refers to the system that coordinates the processes in real time.



BASIC SCADA DIAGRAM

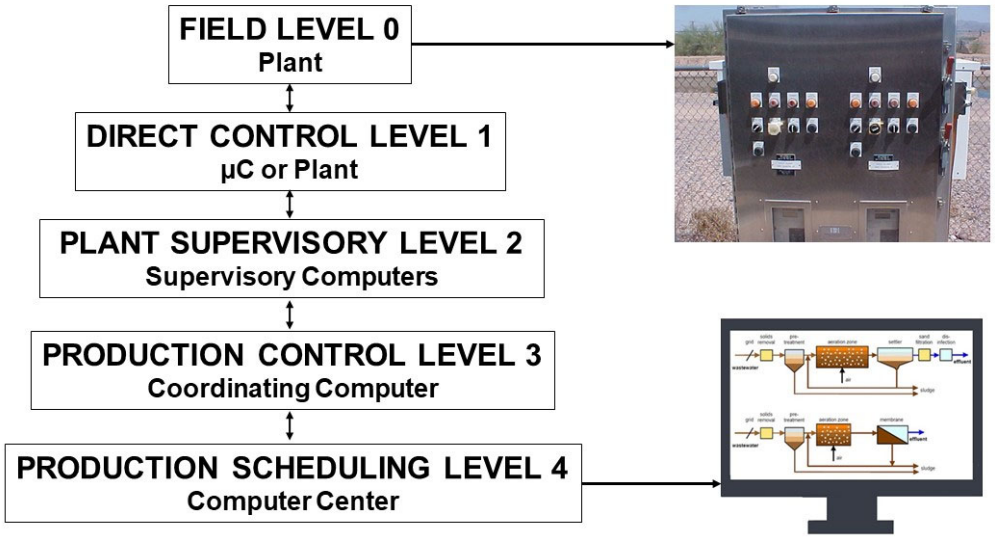
Remote Operation

SCADA is a real time control tool. It is not supposed to be a tool for detailed analysis of past performance but you the operator are able to research past performance to be able to react to current conditions. Thus, some form of trending is included with SCADA. The trending function is as close to analysis as most SCADA software get.

Let us say a water treatment operator wants to examine chemical usage in GAC filters and determine how each filter behaved over the past six weeks. In this case, SCADA is your tool of choice.

Some SCADA let you look at these three filters and compare their performance with some time period in the past.

SCADA Systems Concepts



Technical Learning College

FUNCTION LEVELS OF CONTROL OPERATION

SCADA refers to the centralized systems that control and monitor the entire sites, or they are the complex systems spread out over large areas. Nearly all the control actions are automatically performed by the remote terminal units (RTUs) or by the programmable logic controllers (PLCs). The restrictions to the host control functions are supervisory level intervention or basic overriding. For example, the PLC (in an industrial process) controls the flow of cooling water, the SCADA system allows any changes related to the alarm conditions and set points for the flow (such as high temperature, loss of flow, etc.) to be recorded and displayed.

Data acquisition starts at the PLC or RTU level, which includes the equipment status reports, and meter readings. Data is then formatted in such way that the operator of the control room can make the supervisory decisions to override or adjust normal PLC (RTU) controls, by using the HMI.

SCADA systems mostly implement the distributed databases known as tag databases, containing data elements called points or tags. A point is a single output or input value controlled or monitored by the system. Points are either ‘soft’ or ‘hard’.

The actual output or input of a system is represented by a hard point, whereas the soft point is a result of different math and logic operations applied to other points. These points are usually stored as timestamp-value pairs.

Series of the timestamp-value pairs gives history of the particular point. Storing additional metadata with the tags is common (these additional data can include comments on the design time, alarm information, path to the field device or the PLC register).

The key attribute of a SCADA system is its ability to perform a supervisory operation over a variety of other proprietary devices.

The accompanying diagram is a general model which shows functional manufacturing levels using computerised control.

SCADA systems typically use a tag database, which contains data elements called tags or points, which relate to specific instrumentation or actuators within the process system according to such as the Piping and instrumentation diagram.

Data is accumulated against these unique process control equipment tag references.

Referring to the diagram,
Level 0 contains the field devices such as flow and temperature sensors, and final control elements, such as control valves.
Level 1 contains the industrialised input/output (I/O) modules, and their associated distributed electronic processors.
Level 2 contains the supervisory computers, which collate information from processor nodes on the system, and provide the operator control screens.
Level 3 is the production control level, which does not directly control the process, but is concerned with monitoring production and targets.
Level 4 is the production scheduling level.

Level 1 contains the programmable logic controllers (PLCs) or remote terminal units (RTUs).

Level 2 contains the SCADA software and computing platform. The SCADA software exists only at this supervisory level as control actions are performed automatically by RTUs or PLCs. SCADA control functions are usually restricted to basic overriding or supervisory level intervention.

For example, a PLC may control the flow of cooling water through part of an industrial process to a set point level, but the SCADA system software will allow operators to change the set points for the flow.

The SCADA also enables alarm conditions, such as loss of flow or high temperature, to be displayed and recorded. A feedback control loop is directly controlled by the RTU or PLC, but the SCADA software monitors the overall performance of the loop.

Levels 3 and 4 are not strictly process control in the traditional sense, but are where production control and scheduling takes place.

Data acquisition begins at the RTU or PLC level and includes instrumentation readings and equipment status reports that are communicated to level 2 SCADA as required.

Data is then compiled and formatted in such a way that a control room operator using the HMI (Human Machine Interface) can make supervisory decisions to adjust or override normal RTU (PLC) controls. Data may also be fed to a historian, often built on a commodity database management system, to allow trending and other analytical auditing.

Considerations of SCADA System

Typical considerations when putting a SCADA system together are:

- Overall control requirements
- Sequence logic
- Analog loop control
- Ratio and number of analog to digital points
- Speed of control and data acquisition
- Master/operator control stations
- Type of displays required
- Historical archiving requirements
- System consideration
- Reliability/availability
- Speed of communications/update time/system scan rates
- System redundancy
- Expansion capability
- Application software and modeling

Benefits of a SCADA System

Obviously, a SCADA system's initial cost has to be justified.

A few typical reasons for implementing a SCADA system are:

1. Improved operation of the plant or process resulting in savings due to optimization of the system
2. Increased productivity of the personnel
3. Improved safety of the system due to better information and improved control
4. Protection of the plant equipment
5. Safeguarding the environment from a failure of the system
6. Improved energy savings due to optimization of the plant
7. Improved and quicker receipt of data so that clients can be invoiced more quickly and accurately
8. Government regulations for safety and metering of gas (for royalties etc.)

Human Machine Interface Introduction

The HMI, or Human Machine Interface, is an apparatus that gives the processed data to the human operator. A human operator uses HMI to control processes.

The HMI is linked to the SCADA system's databases, to provide the diagnostic data, management information and trending information such as logistic information, detailed schematics for a certain machine or sensor, maintenance procedures and troubleshooting guides.

The information provided by the HMI to the operating personnel is graphical, in the form of mimic diagrams. This means the schematic representation of the plant that is being controlled is available to the operator.

For example, a photograph of the pump that is connected to the pipe shows that this pump is running and it also shows the amount of fluid pumping through the pipe at the particular moment. The pump can then be switched off by the operator.

The software of the HMI shows the decrease in the flow rate of fluid in the pipe in the real time. Mimic diagrams either consist of digital photographs of process equipment with animated symbols, or schematic symbols and line graphics that represent various process elements.

HMI package of the SCADA systems consist of a drawing program used by the system maintenance personnel or operators to change the representation of these points in the interface.

These representations can be as simple as on-screen traffic light that represents the state of the actual traffic light in the area, or complex, like the multi-projector display that represents the position of all the trains on railway or elevators in skyscraper.

SCADA systems are commonly used in alarm systems. The alarm has only two digital status points with values ALARM or NORMAL.

When the requirements of the Alarm are met, the activation will start. For example, when the fuel tank of a car is empty, the alarm is activated and the light signal is on. To alert the SCADA operators and managers, text messages and emails are sent along with alarm activation.

Supervisory Station Introduction

A ‘supervisory Station’ refers to the software and servers responsible for communication with the field equipment (PLCs, RTUs etc.), and after that, to HMI software running on the workstations in the control room, or somewhere else.

A master station can be composed of only one PC (in small SCADA systems). Master station can have multiple servers, disaster recovery sites and distributed software applications in larger SCADA systems. For increasing the system integrity, multiple servers are occasionally configured in hot standby or dual-redundant formation, providing monitoring and continuous control during server failures.

SCADA Hardware

SCADA system may have the components of the Distributed Control System. Execution of easy logic processes without involving the master computer is possible because ‘smart’ PLCs or RTUs. IEC61131-39(Ladder Logic) is used, (this is a functional block programming language, commonly used in creating programs running on PLCs and RTUs.) IEC 61131-3 has very few training requirements, unlike procedural languages like FORTRAN and C programming language.

The SCADA system engineers can perform implementation and design of programs being executed on PLC or RTU. The compact controller, Programmable automation controller (PAC), combines the capabilities and features of a PC-based control system with a typical PLC.

’Distributed RTUs’, in various electrical substation SCADA applications, use station computers or information processors for communicating with PACs, protective relays, and other I/O devices. Almost all big PLC manufacturers offer integrated HMI/SCADA systems, since 1998. Many of them are using non-proprietary and open communication protocols.

Many skilled third party HMI/SCADA packages have stepped into the market, offering in-built compatibility with several major PLCs, which allows electrical engineers, mechanical engineers or technicians to configure HMIs on their own, without requiring software-developer-written custom-made program.

Remote Terminal Unit (RTU)

The RTU is connected to the physical equipment. Often, the RTU converts all electrical signals coming from the equipment into digital values like the status- open/closed – from a valve or switch, or the measurements like flow, pressure, current or voltage. By converting and sending the electrical signals to the equipment, RTU may control the equipment, like closing or opening a valve or a switch, or setting the speed of the pump.

SCADA Operational Philosophy

The costs resulting from control system failures are very high. Even lives may be lost. For a few SCADA systems, hardware is ruggedized, to withstand temperature, voltage and vibration extremes, and reliability is increased, in many critical installations, by including communications channels and redundant hardware. A part which is failing can be identified and the functionality taken over automatically through backup hardware. It can be replaced without any interruption of the process.

Communication Methods and Infrastructure
SCADA systems initially used modem connections or combinations of direct and radio serial to meet communication requirements, even though IP and Ethernet over SONET/SDH can also be used at larger sites like power stations and railways. The monitoring function or remote management of the SCADA system is called telemetry.

SCADA protocols have been designed to be extremely compact and to send information to the master station only when the RTU is polled by the master station. Typically, the legacy of SCADA protocols consists of Conitel, Profibus, Modbus RTU and RP-570. These protocols of communication are specifically SCADA-vendor. Standard protocols are IEC 61850, DNP3 and IEC 60870-5-101 or 104. These protocols are recognized and standardized by all big SCADA vendors. Several of these protocols have extensions for operating through the TCP/IP.

The development of many automatic controller devices and RTUs had started before the advent of industry standards for the interoperability.

For better communication between different software and hardware, PLE for Process Control is a widely accepted solution that allows communication between the devices that originally weren’t intended to be part of the industrial network.

Alarm Management Introduction
An important part of most SCADA implementations is alarm handling. The system monitors whether certain alarm conditions are satisfied, to determine when an alarm event has occurred. Once an alarm event has been detected, one or more actions are taken (such as the activation of one or more alarm indicators, and perhaps the generation of email or text messages so that management or remote SCADA operators are informed).

In many cases, a SCADA operator may have to acknowledge the alarm event; this may deactivate some alarm indicators, whereas other indicators remain active until the alarm conditions are cleared.

Alarm conditions can be explicit—for example, an alarm point is a digital status point that has either the value NORMAL or ALARM that is calculated by a formula based on the values in other analogue and digital points—or implicit: the SCADA system might automatically monitor whether the value in an analogue point lies outside high and low- limit values associated with that point.

Examples of alarm indicators include a siren, a pop-up box on a screen, or a colored or flashing area on a screen (that might act in a similar way to the "fuel tank empty" light in a car); in each case, the role of the alarm indicator is to draw the operator's attention to the part of the system 'in alarm' so that appropriate action can be taken.

PLC/RTU Programming
"Smart" RTUs, or standard PLCs, are capable of autonomously executing simple logic processes without involving the supervisory computer. They employ standardized control programming languages such as under, IEC 61131-3 (a suite of 5 programming languages including function block, ladder, structured text, sequence function charts and instruction list), is frequently used to create programs which run on these RTUs and PLCs.

Unlike a procedural language such as the C programming language or FORTRAN, IEC 61131-3 has minimal training requirements by virtue of resembling historic physical control arrays. This allows SCADA system engineers to perform both the design and implementation of a program to be executed on an RTU or PLC.

A programmable automation controller (PAC) is a compact controller that combines the features and capabilities of a PC-based control system with that of a typical PLC. PACs are deployed in SCADA systems to provide RTU and PLC functions.

In many electrical substation SCADA applications, "distributed RTUs" use information processors or station computers to communicate with digital protective relays, PACs, and other devices for I/O, and communicate with the SCADA master in lieu of a traditional RTU.

PLC Commercial Integration
Since about 1998, virtually all major PLC manufacturers have offered integrated HMI/SCADA systems, many of them using open and non-proprietary communications protocols.

Numerous specialized third-party HMI/SCADA packages, offering built-in compatibility with most major PLCs, have also entered the market, allowing mechanical engineers, electrical engineers and technicians to configure HMIs themselves, without the need for a custom-made program written by a software programmer.

The Remote Terminal Unit (RTU) connects to physical equipment. Typically, an RTU converts the electrical signals from the equipment to digital values such as the open/closed status from a switch or a valve, or measurements such as pressure, flow, voltage or current. By converting and sending these electrical signals out to equipment the RTU can control equipment, such as opening or closing a switch or a valve, or setting the speed of a pump.

SCADA Architectures

Monolithic: The First Generation
In the first generation, mainframe systems were used for computing. At the time SCADA was developed, networks did not exist. Therefore, the SCADA systems did not have any connectivity to other systems, meaning they were independent systems. Later on, RTU vendors designed the Wide Area Networks that helped in communication with RTU. The usage of communication protocols at that time was proprietary. If the mainframe system failed, there was a back-up mainframe, connected at the bus level.

Distributed: The Second Generation
The information between multiple stations was shared in real time through LAN and the processing was distributed between various multiple stations. The cost and size of the stations were reduced in comparison to the ones used in the first generation. The protocols used for the networks were still proprietary, which caused many security issues for SCADA systems. Due to the proprietary nature of the protocols, very few people actually knew how secure the SCADA installation was.

Networked: The Third Generation
The SCADA system used today belong to this generation. The communication between the system and the master station is done through the WAN protocols like the Internet Protocols (IP). Since the standard protocols used and the networked SCADA systems can be accessed through the internet, the vulnerability of the system is increased. However, the usage of security techniques and standard protocols means that security improvements can be applied in SCADA systems.

The Evolution of SCADA
The first iteration of SCADA started off with mainframe computers. Networks as we know them today were not available and each SCADA system stood on its own. These systems were what would now be referred to as monolithic SCADA systems.

In the 80s and 90s, SCADA continued to evolve thanks to smaller computer systems, Local Area Networking (LAN) technology, and PC-based HMI software. SCADA systems soon were able to be connected to other similar systems. Many of the LAN protocols used in these systems were proprietary, which gave vendors control of how to optimize data transfer. Unfortunately, these systems were incapable of communicating with systems from other vendors. These systems were called distributed SCADA systems.

In the 1990s and early 2000s, building upon the distributed system model, SCADA adopted an incremental change by embracing an open system architecture and communications protocols that were not vendor-specific. This iteration of SCADA, called a networked SCADA system, took advantage of communications technologies such as Ethernet. Networked SCADA systems allowed systems from other vendors to communicate with each other, alleviating the limitations imposed by older SCADA systems, and allowed organizations to connect more devices to the network.

While SCADA systems have undergone substantial evolutionary changes, many industrial organizations continued to struggle with industrial data access from the enterprise level. By the late 1990s to the early 2000s, a technological boom occurred and personal computing and IT technologies accelerated in development.

Structured query language (SQL) databases became the standard for IT databases but were not adopted by SCADA developers. This resulted in a rift between the fields of controls and IT, and SCADA technology became antiquated over time.

Traditional SCADA systems still use proprietary technology to handle data. Whether it is a data historian, a data connector, or other means of data transfer, the solution is messy and incredibly expensive. Modern SCADA systems aim to solve this problem by leveraging the best of controls and IT technology.

Communication Infrastructure and Methods

SCADA systems have traditionally used combinations of radio and direct wired connections, although SONET/SDH is also frequently used for large systems such as railways and power stations. The remote management or monitoring function of a SCADA system is often referred to as telemetry. Some users want SCADA data to travel over their pre-established corporate networks or to share the network with other applications. The legacy of the early low-bandwidth protocols remains, though.

SCADA protocols are designed to be very compact. Many are designed to send information only when the master station polls the RTU. Typical legacy SCADA protocols include Modbus RTU, RP-570, Profibus and Conitel. These communication protocols, with the exception of Modbus (Modbus has been made open by Schneider Electric), are all SCADA-vendor specific but are widely adopted and used. Standard protocols are IEC 60870-5-101 or 104, IEC 61850 and DNP3. These communication protocols are standardized and recognized by all major SCADA vendors. Many of these protocols now contain extensions to operate over TCP/IP. Although the use of conventional networking specifications, such as TCP/IP, blurs the line between traditional and industrial networking, they each fulfill fundamentally differing requirements. Network simulation can be used in conjunction with SCADA simulators to perform various 'what-if' analyses.

With increasing security demands (such as North American Electric Reliability Corporation (NERC) and critical infrastructure protection (CIP) in the US), there is increasing use of satellite-based communication. This has the key advantages that the infrastructure can be self-contained (not using circuits from the public telephone system), can have built-in encryption, and can be engineered to the availability and reliability required by the SCADA system operator. Earlier experiences using consumer-grade VSAT were poor. Modern carrier-class systems provide the quality of service required for SCADA.

RTUs and other automatic controller devices were developed before the advent of industry wide standards for interoperability. The result is that developers and their management created a multitude of control protocols. Among the larger vendors, there was also the incentive to create their own protocol to "lock in" their customer base. A list of automation protocols is compiled here.

OLE for process control (OPC) can connect different hardware and software, allowing communication even between devices originally not intended to be part of an industrial network. Standardisation in the field of mySCADA protocols resulted into the vendor independent protocol called OPC UA (Unified Architecture). OPC UA is starting to be widely adopted among multiple SCADA vendors.

SCADA Trends
In the late 1990s instead of using the RS-485, manufacturers used open message structures like Modbus ASCII and Modbus RTU (both developed by Modicon). By 2000, almost all I/O makers offered fully open interfacing like Modbus TCP instead of the IP and Ethernet.

SCADA systems are now in line with the standard networking technologies. The old proprietary standards are being replaced by the TCP/IP and Ethernet protocols. However, due to certain characteristics of frame-based network communication technology, Ethernet networks have been accepted by the majority of markets for HMI SCADA.

The 'Next Generation' protocols using XML web services and other modern web technologies, make themselves more IT supportable. A few examples of these protocols include Wonderware's SuiteLink, GE Fanuc's Proficy, I Gear's Data Transport Utility, Rockwell Automation's FactoryTalk and OPC-UA.

Some vendors have started offering application-specific SCADA systems that are hosted on remote platforms all over the Internet. Hence, there is no need to install systems at the user-end facility. Major concerns are related to the Internet connection reliability, security and latency.
The SCADA systems are becoming omnipresent day by day. However, there are still some security issues.

SCADA Security Issues
Security of SCADA-based systems is being questioned, as they are potential targets to cyberterrorism/cyberwarfare attacks.

There is an erroneous belief that SCADA networks are safe enough because they are secured physically. It is also wrongly believed that SCADA networks are safe enough because they are disconnected from the Internet.

SCADA systems also are used for monitoring and controlling physical processes, like distribution of water, traffic lights, electricity transmissions, gas transportation and oil pipelines and other systems used in the modern society. Security is extremely important because destruction of the systems would have very bad consequences.

There are two major threats. The first one is unauthorized access to software, be it human access or intentionally induced changes, virus infections or other problems that can affect the control host machine. The second threat is related to the packet access to network segments that host SCADA devices. In numerous cases, there remains less or no security on actual packet control protocol; therefore, any person sending packets to SCADA device is in position to control it. Often, SCADA users infer that VPN is sufficient protection, and remain oblivious to the fact that physical access to network switches and jacks related to SCADA provides the capacity to bypass the security on control software and control SCADA networks.

SCADA vendors are addressing these risks by developing specialized industrial VPN and firewall solutions for SCADA networks that are based on TCP/IP. In addition, white-listing solutions have been implemented due to their ability to prevent unauthorized application changes.

SCADA systems that tie together decentralized facilities such as power, oil, gas pipelines, water distribution and wastewater collection systems were designed to be open, robust, and easily operated and repaired, but not necessarily secure.

The move from proprietary technologies to more standardized and open solutions together with the increased number of connections between SCADA systems, office networks and the Internet has made them more vulnerable to types of network attacks that are relatively common in computer security. For example, United States Computer Emergency Readiness Team (US-CERT) released a vulnerability advisory warning that unauthenticated users could download sensitive configuration information including password hashes from an Inductive Automation Ignition system utilizing a standard attack type leveraging access to the Tomcat Embedded Web server. Security researcher Jerry Brown submitted a similar advisory regarding a buffer overflow vulnerability in a Wonderware InBatchClient ActiveX control. Both vendors made updates available prior to public vulnerability release. Mitigation recommendations were standard patching practices and requiring VPN access for secure connectivity. Consequently, the security of some SCADA-based systems has come into question as they are seen as potentially vulnerable to cyber attacks.

In particular, security researchers are concerned about

- the lack of concern about security and authentication in the design, deployment and operation of some existing SCADA networks
- the belief that SCADA systems have the benefit of security through obscurity through the use of specialized protocols and proprietary interfaces
- the belief that SCADA networks are secure because they are physically secured
- the belief that SCADA networks are secure because they are disconnected from the Internet

SCADA systems are used to control and monitor physical processes, examples of which are transmission of electricity, transportation of gas and oil in pipelines, water distribution, traffic lights, and other systems used as the basis of modern society. The security of these SCADA systems is important because compromise or destruction of these systems would impact multiple areas of society far removed from the original compromise. For example, a blackout caused by a compromised electrical SCADA system would cause financial losses to all the customers that received electricity from that source. How security will affect legacy SCADA and new deployments remains to be seen.

There are many threat vectors to a modern SCADA system. One is the threat of unauthorized access to the control software, whether it is human access or changes induced intentionally or accidentally by virus infections and other software threats residing on the control host machine. Another is the threat of packet access to the network segments hosting SCADA devices. In many cases, the control protocol lacks any form of cryptographic security, allowing an attacker to control a SCADA device by sending commands over a network.

In many cases, SCADA users have assumed that having a VPN offered sufficient protection, unaware that security can be trivially bypassed with physical access to SCADA-related network jacks and switches. Industrial control vendors suggest approaching SCADA security like Information Security with a defense in depth strategy that leverages common IT practices

The reliable function of SCADA systems in our modern infrastructure may be crucial to public health and safety. As such, attacks on these systems may directly or indirectly threaten public health and safety. Such an attack has already occurred, carried out on Maroochy Shire Council's sewage control system in Queensland, Australia. Shortly after a contractor installed a SCADA system in January 2000, system components began to function erratically. Pumps did not run when needed and alarms were not reported.

More critically, sewage flooded a nearby park and contaminated an open surface-water drainage ditch and flowed 500 meters to a tidal canal. The SCADA system was directing sewage valves to open when the design protocol should have kept them closed. Initially this was believed to be a system bug.

Monitoring of the system logs revealed the malfunctions were the result of cyber attacks. Investigators reported 46 separate instances of malicious outside interference before the culprit was identified. The attacks were made by a disgruntled ex-employee of the company that had installed the SCADA system. The ex-employee was hoping to be hired by the utility full-time to maintain the system.

In April 2008, the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack issued a Critical Infrastructures Report which discussed the extreme vulnerability of SCADA systems to an electromagnetic pulse (EMP) event. After testing and analysis, the Commission concluded: "SCADA systems are vulnerable to an EMP event.

The large numbers and widespread reliance on such systems by all of the Nation’s critical infrastructures represent a systemic threat to their continued operation following an EMP event. Additionally, the necessity to reboot, repair, or replace large numbers of geographically widely dispersed systems will considerably impede the Nation’s recovery from such an assault."

Summary

SCADA System

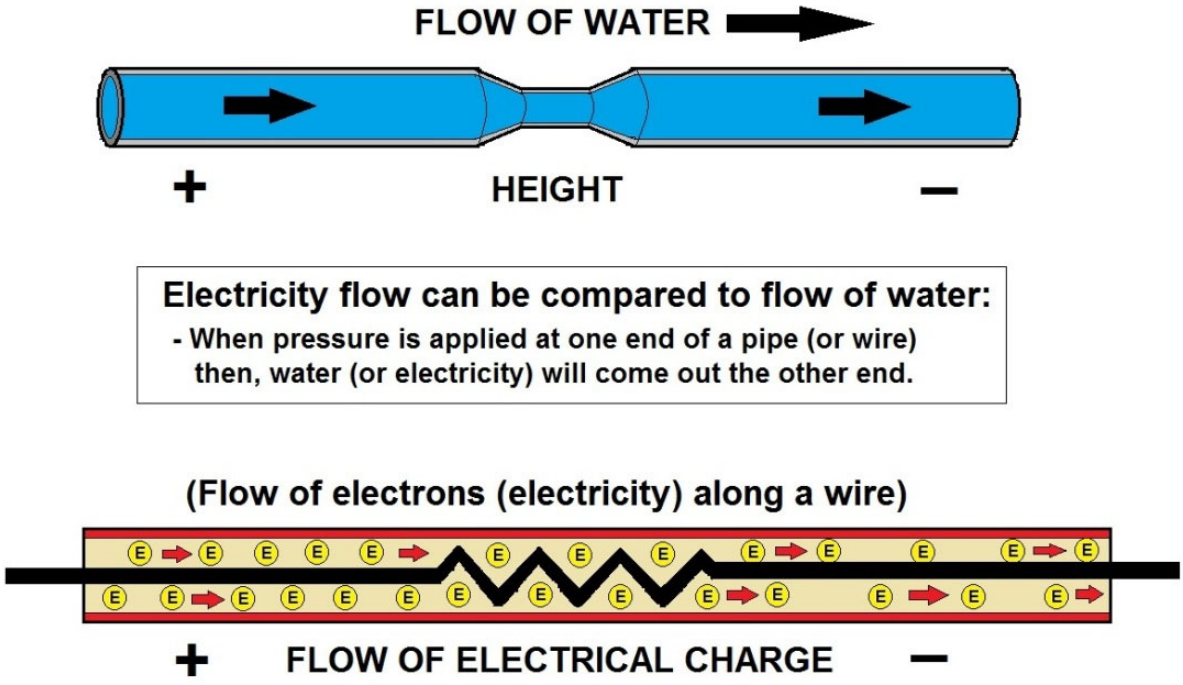
A SCADA (or supervisory control and data acquisition) system means a system consisting of a number of remote terminal units (or RTUs) collecting field data connected back to a master station via a communications system.

The master station displays the acquired data and allows the operator to perform remote control tasks.

The accurate and timely data (normally real-time) allows for optimization of the operation of the plant and process. A further benefit is more efficient, reliable and most importantly, safer operations. This all results in a lower cost of operation compared to earlier non-automated systems.

There is a fair degree of confusion between the definition of SCADA systems and process control system. SCADA has the connotation of remote or distant operation.

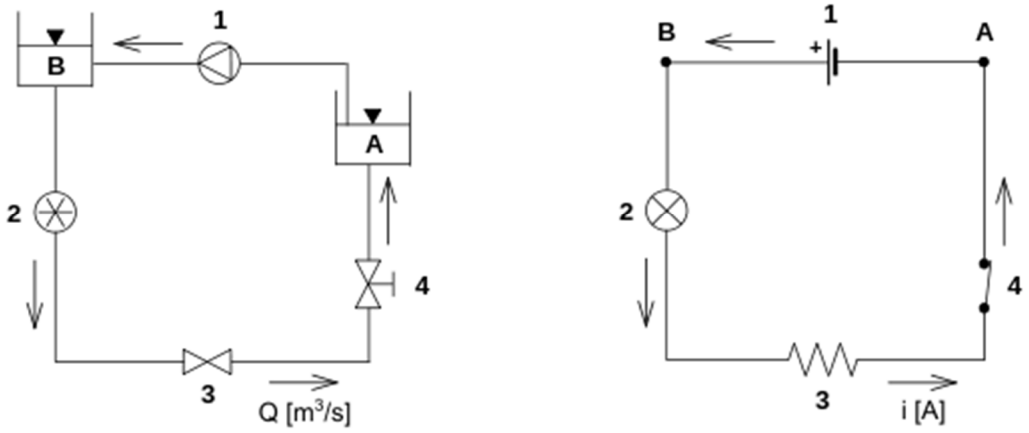
Hydraulic Analogy Principles Section



Water (Hydraulic) and Electrical Principles Are Very Similar

The electronic–**hydraulic analogy** (derisively referred to as the **drain-pipe theory** by Oliver Heaviside) is the most widely used analogy for "electron fluid" in a metal conductor. Since electric current is invisible and the processes at play in electronics are often difficult to demonstrate, the various electronic components are represented by hydraulic equivalents.

Electricity (as well as heat) was originally understood to be a kind of fluid, and the names of certain electric quantities (such as current) are derived from hydraulic equivalents. As all analogies, it demands an intuitive and competent understanding of the baseline paradigms (electronics and hydraulics).



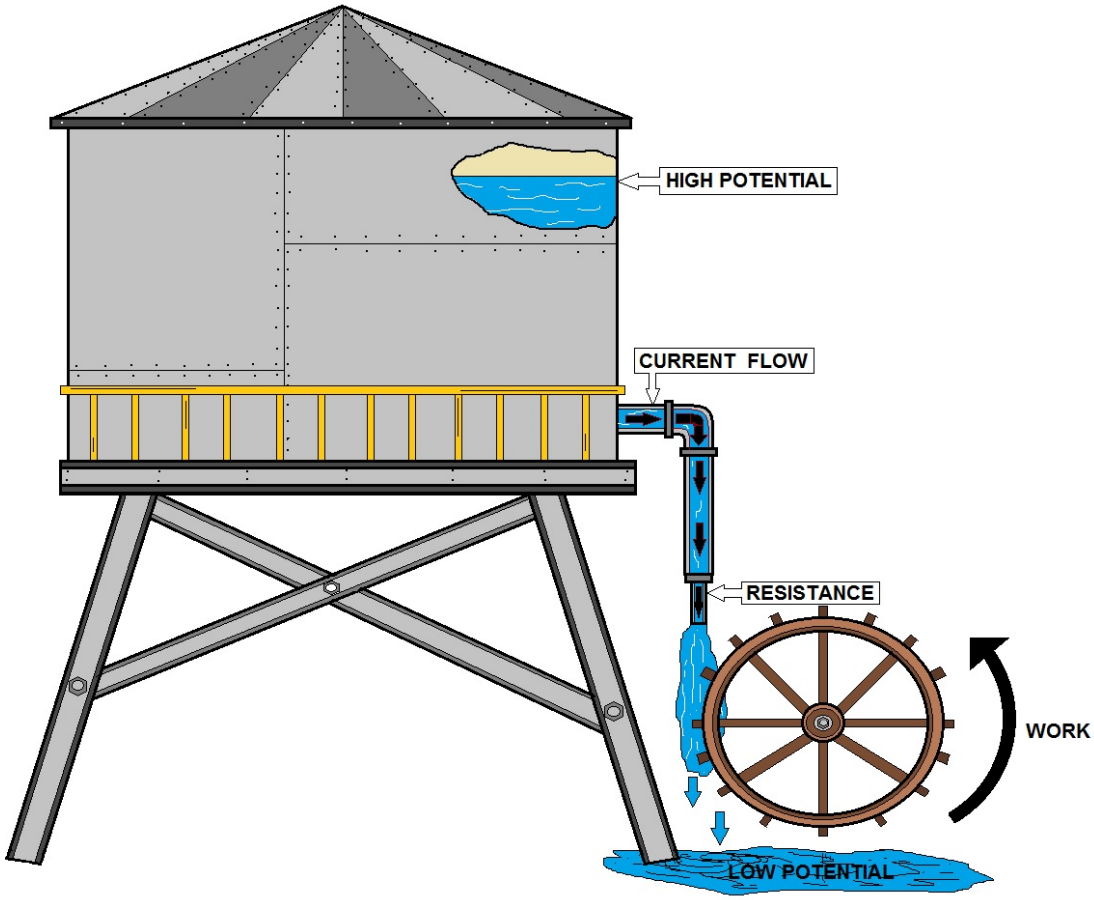
Analogy between a hydraulic circuit (left) and an electronic circuit (right).

Basic Hydraulic Ideas

There are two basic paradigms:

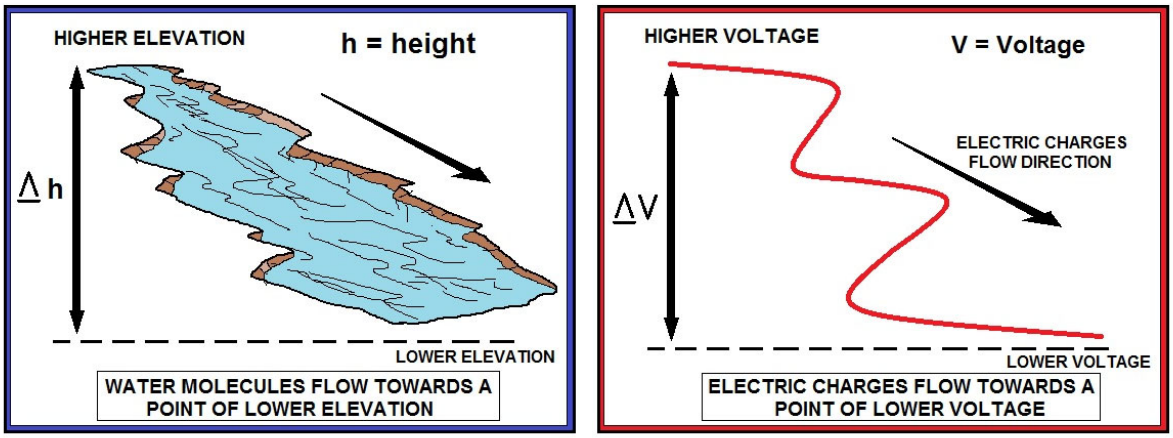
- Version with pressure induced by gravity. Large tanks of water are held up high, or are filled to differing water levels, and the potential energy of the water head is the pressure source. This is reminiscent of electrical diagrams with an up arrow pointing to +V, grounded pins that otherwise are not shown connecting to anything, and so on.
- Completely enclosed version with pumps providing pressure only; no gravity. This is reminiscent of a circuit diagram with a voltage source shown and the wires actually completing a circuit.

Applications: Flow and pressure variables can be calculated in fluid flow network with the use of the hydraulic ohm analogy. The method can be applied to both steady and transient flow situations.



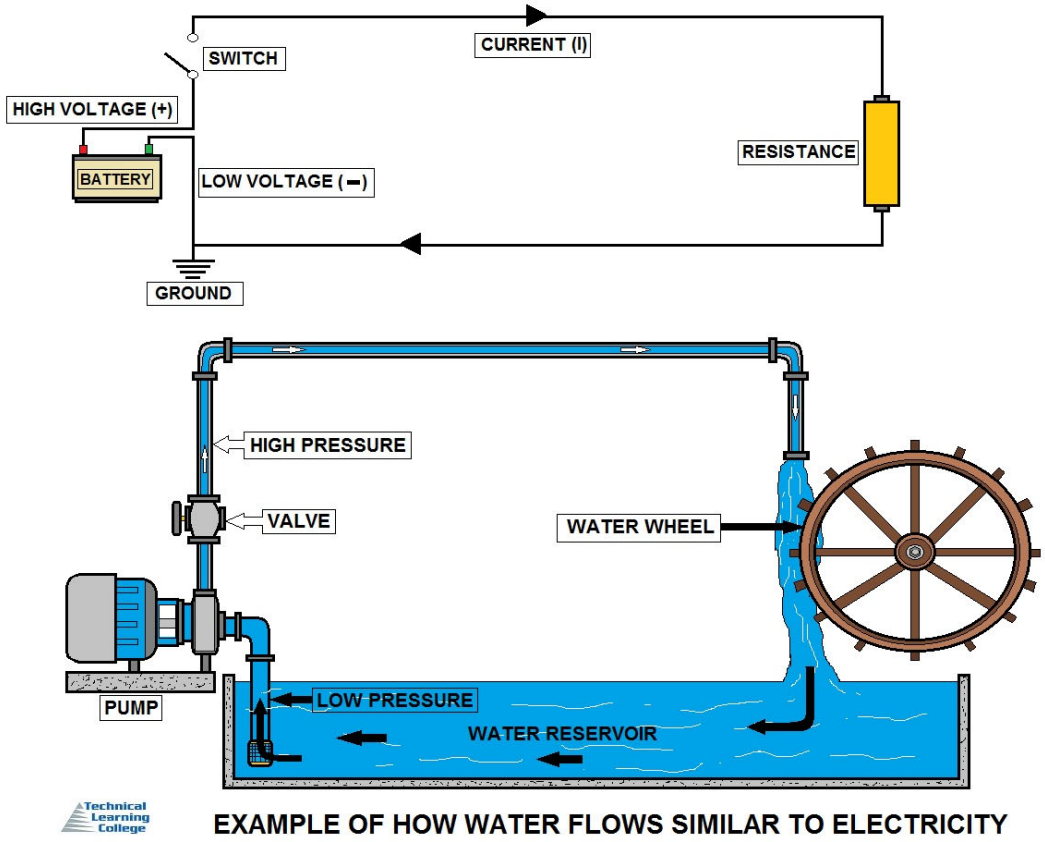
Technical Learning College

WATER FLOWS LIKE ELECTRICITY



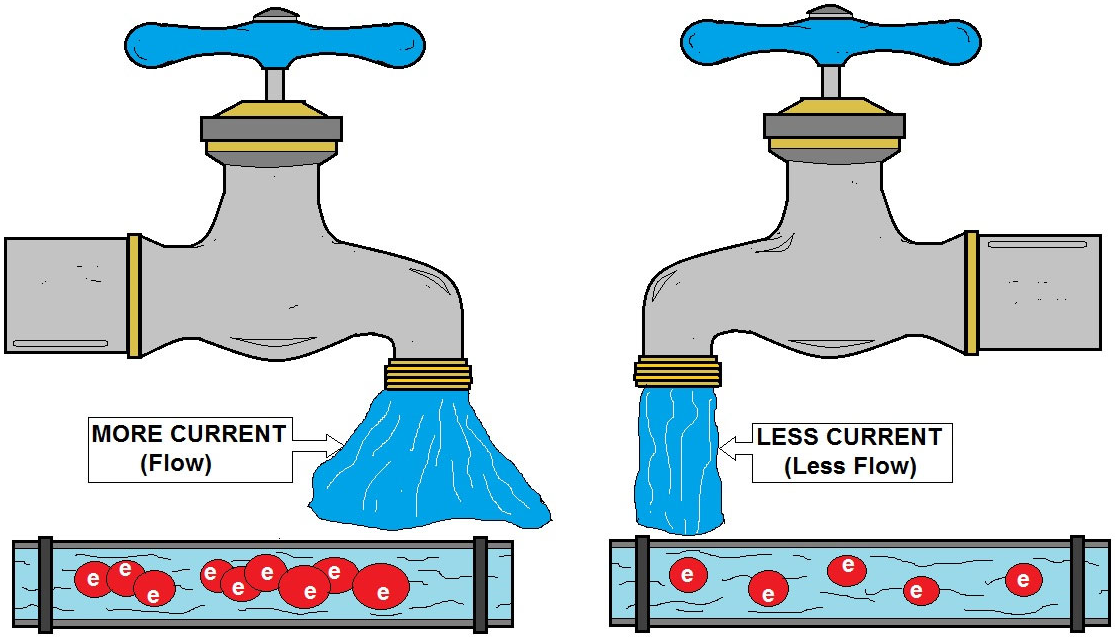
Technical Learning College

WATER FLOWS LIKE ELECTRICITY EXAMPLE



Technical Learning College

EXAMPLE OF HOW WATER FLOWS SIMILAR TO ELECTRICITY



Technical Learning College

ELECTRIC CURRENT - WATER ANALOGY

Hydraulic Component Equivalents

Wires
A relatively wide pipe completely filled with water is equivalent to a piece of wire. When comparing to a piece of wire, the pipe should be thought of as having semi-permanent caps on the ends. Connecting one end of a wire to a circuit is equivalent to forcibly un-capping one end of the pipe and attaching it to another pipe. With few exceptions (such as a high-voltage power source), a wire with only one end attached to a circuit will do nothing; the pipe remains capped on the free end, and thus adds nothing to the circuit.

Electric Potential
In general, it is equivalent to hydraulic head. In this article, it is assumed that the water is flowing horizontally, so that the force of gravity can be ignored, and then electric potential is equivalent to pressure.

Voltage
Also called voltage drop or *potential difference*. A difference in pressure between two points. Usually measured in volts.

Electric charge
Equivalent to a quantity of water.

Current
Equivalent to a hydraulic volume flow rate; that is, the volumetric quantity of flowing water over time. Usually measured in amperes.

Ideal voltage source, or ideal battery
A dynamic pump with feedback control. A pressure meter on both sides shows that regardless of the current being produced, this kind of pump produces constant pressure difference. If one terminal is kept fixed at ground, another analogy is a large body of water at a high elevation, sufficiently large that the drawn water does not affect the water level.

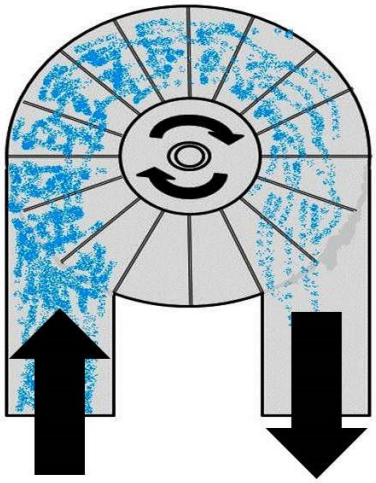
Ideal current source
A positive displacement pump. A current meter (little paddle wheel) shows that when this kind of pump is driven at a constant speed, it maintains a constant speed of the little paddle wheel.

Resistor
A constriction in the bore of the pipe which requires more pressure to pass the same amount of water. All pipes have some resistance to flow, just as all wires have some resistance to current.

Capacitor
A tank with one connection at each end and a rubber sheet dividing the tank in two lengthwise (a hydraulic accumulator). When water is forced into one pipe, equal water is simultaneously forced out the other pipe, yet no water can penetrate the rubber diaphragm. Energy is stored by the stretching of the rubber. As more current flows "through" the capacitor, the back-pressure (voltage) becomes greater, thus current "leads" voltage in a capacitor. As the back-pressure from the stretched rubber approaches the applied pressure, the current becomes less and less. Thus capacitors "filter out" constant pressure differences and slowly varying, low-frequency pressure differences, while allowing rapid changes in pressure to pass through.

Note that the device described will pass all changes in pressure "through" equally well, regardless of rate of change, just as an electrical capacitor will. Any device in series must obey (electrical) Kirchhoff's Current Law, or its hydraulic equivalent. Considering the "filter" action, a better and more exact analogy is the hydraulic accumulator "pressure tank", as described, but with a closed, pressurized air bladder and only one water connection. Such accumulators are commonly used in hydraulic power systems exactly for the purpose of damping out pressure surges and "hammers" due to valves opening and closing.

Inductor
A heavy paddle wheel placed in the current. The mass of the wheel and the size of the blades restrict the water's ability to rapidly change its rate of flow (current) through the wheel due to the effects of inertia, but, given time, a constant flowing stream will pass mostly unimpeded through the wheel, as it turns at the same speed as the water flow. The mass and surface area of the wheel and its blades are analogous to inductance, and friction between its axle and the axle bearings corresponds to the resistance that accompanies any non-superconducting inductor.



TURBINE INDUCTOR PADDLE

Inductors are analogous to a heavy paddle wheel/turbine placed in the current.

An alternative inductor model is simply a long pipe, perhaps coiled into a spiral for convenience. This fluid-inertia device is used in real life as an essential component of a hydraulic ram. The inertia of the water flowing through the pipe produces the inductance effect; inductors "filter out" rapid changes in flow, while allowing slow variations in current to be passed through. The drag imposed by the walls of the pipe is somewhat analogous to parasitic resistance.

In either model, the pressure difference (voltage) across the device must be present before the current will start moving, thus in inductors voltage "leads" current. As the current increases, approaching the limits imposed by its own internal friction and of the current that the rest of the circuit can provide, the pressure drop across the device becomes lower and lower.

Diode
Equivalent to a one-way check valve with a slightly leaky valve seat. As with a diode, a small pressure difference is needed before the valve opens. And like a diode, too much reverse bias can damage or destroy the valve assembly.

Transistor
A valve in which a diaphragm, controlled by a low-current signal (either constant current for a BJT or constant pressure for a FET), moves a plunger which affects the current through another section of pipe.

CMOS
A combination of two MOSFET transistors. As the input pressure changes, the pistons allow the output to connect to either zero or positive pressure.

Memristor
A needle valve operated by a flow meter. As water flows through in the forward direction, the needle valve restricts flow more; as water flows the other direction, the needle valve opens further providing less resistance.

Hydraulic - Electrical Principle Equivalents

EM Wave Speed (velocity of propagation)
Speed of sound in water. When a light switch is flipped, the electric wave travels very quickly through the wires.

Charge Flow Speed (drift velocity)
Particle speed of water. The moving charges themselves move rather slowly.

DC
Constant flow of water in a circuit of pipe.

Low Frequency AC
Water oscillating back and forth in a pipe.

Higher-Frequency AC and Transmission Lines
Sound being transmitted through the water pipes: Be aware that this does not properly mirror the cyclical reversal of alternating electric current. As described, the fluid flow conveys pressure fluctuations, but fluids “do not” reverse at high rates in hydraulic systems, which the above "low frequency" entry does accurately describe. A better concept (if sound waves are to be the phenomenon) is that of direct current with high-frequency "ripple" superimposed.

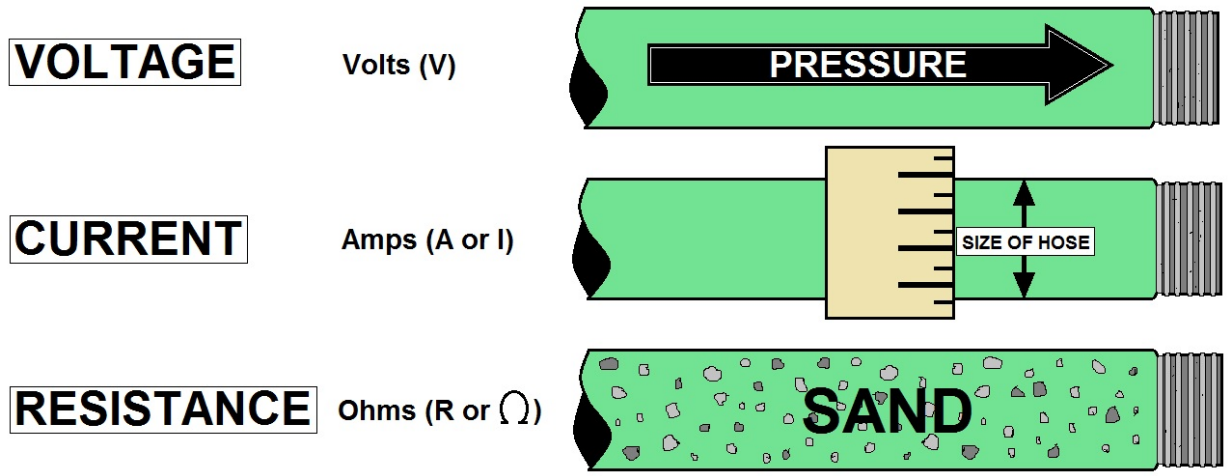
Inductive Spark
Used in induction coils, similar to water hammer, caused by the inertia of water.

Hydraulic Equation Examples

Some examples of equivalent electrical and hydraulic equations:

type	hydraulic	electric	thermal	mechanical
quantity	volume V [m³]	charge q [C]	heat Q [J]	momentum P [Ns]
potential	pressure p [Pa=J/m³]	potential ϕ [V=J/C]	temperature T [K=J/k_B]	velocity v [m/s]
flux	Volumetric flow rate Φ_V [m³/s]	current I [A=C/s]	heat transfer rate $\dot{Q}$ [J/s]	force F [N]
flux density	velocity v [m/s]	current density j [C/(m²·s) = A/m²]	heat flux $\dot{Q}''$ [W/m²]	stress σ [N/m² = Pa]
linear model	Poiseuille's law $\Phi_V = \frac{\pi r^4}{8\eta}\frac{\Delta p^\star}{\ell}$	Ohm's law $j = -\sigma\nabla\phi$	Fourier's law $\dot{Q}'' = \kappa\nabla T$	Dashpot $\sigma = c\Delta v$

If the differential equations have the same form, the response will be similar.



HOW ELECTRICITY IS SIMILAR TO A WATER HOSE

Technical Learning College

Limits to the Hydraulic Analogy

If taken too far, the water analogy can create misconceptions. For it to be useful, we must remain aware of the regions where electricity and water behave very differently.

Fields (Maxwell equations, Inductance)
Electrons can push or pull other distant electrons via their fields, while water molecules experience forces only from direct contact with other molecules. For this reason, waves in water travel at the speed of sound, but waves in a sea of charge will travel much faster as the forces from one electron are applied to many distant electrons and not to only the neighbors in direct contact. In a hydraulic transmission line, the energy flows as mechanical waves through the water, but in an electric transmission line the energy flows as fields in the space surrounding the wires, and does not flow inside the metal. Also, an accelerating electron will drag its neighbors along while attracting them, both because of magnetic forces.

Charge
Unlike water, movable charge carriers can be positive or negative, and conductors can exhibit an overall positive or negative net charge. The mobile carriers in electric currents are usually electrons, but sometimes they are charged positively, such as H^+ ions in proton conductors or holes in p-type semiconductors and some (very rare) conductors.

Leaking Pipes
The electric charge of an electrical circuit and its elements is usually almost equal to zero, hence it is (almost) constant. This is formalized in Kirchhoff's current law, which does not have an analogy to hydraulic systems, where amount of the liquid is not usually constant. Even with incompressible liquid the system may contain such elements as pistons and open pools, so the volume of liquid contained in a part of the system can change. For this reason, continuing electric currents require closed loops rather than hydraulics' open source/sink resembling spigots and buckets.

> **James Thurber spoke of his maternal grandmother thus:**
> *She came naturally by her confused and groundless fears, for her own mother lived the latter years of her life in the horrible suspicion that electricity was dripping invisibly all over the house. - My Life and Hard Times (1933).*

Fluid Velocity and Resistance of Metals
As with water hoses, the carrier drift velocity in conductors is directly proportional to current. However, water only experiences drag via the pipes' inner surface, while charges are slowed at all points within a metal. Also, typical velocity of charge carriers within a conductor is less than centimeters per minute, and the "electrical friction" is extremely high. If charges ever flowed as fast as water can flow in pipes, the electric current would be immense, and the conductors would become incandescently hot and perhaps vaporize.

To model the resistance and the charge-velocity of metals, perhaps a pipe packed with sponge, or a narrow straw filled with syrup, would be a better analogy than a large-diameter water pipe. Resistance in most electrical conductors is a linear function: as current increases, voltage drop increases proportionally (Ohm's Law). Liquid resistance in pipes is not linear with volume, varying as the square of volumetric flow (see Darcy–Weisbach equation).

Quantum Mechanics
Conductors and insulators contain charges at more than one discrete level of atomic orbit energy, while the water in one region of a pipe can only have a single value of pressure. For this reason there is no hydraulic explanation for such things as a battery's charge pumping ability, a diode's voltage drop, solar cell functions, Peltier effect, etc., however equivalent devices can be designed which exhibit similar responses, although some of the mechanisms would only serve to regulate the flow curves rather than to contribute to the component's primary function.

Usefulness requires that the reader or student has a substantial understanding of the model (hydraulic) system's principles. It also requires that the principles can be transferred to the target (electrical) system. Hydraulic systems are deceptively simple: the phenomenon of pump cavitation is a known, complex problem that few people outside of the fluid power or irrigation industries would understand. For those who do, the hydraulic analogy is amusing, as no "cavitation" equivalent exists in electrical engineering. The hydraulic analogy can give a mistaken sense of understanding that will be exposed once a detailed description of electrical circuit theory is required.

One must also consider the difficulties in trying to make the analogy work. The above "electrical friction" example, where the hydraulic analog is a pipe filled with sponge material, illustrates the problem: the model must be increased in complexity beyond any realistic scenario.

Electrical Measurements and Equipment

Molecule of liquid ⟶ electron of electricity

Flow rate (gpm) ⟶ current (ampere) I, A

Pressure (psi) ⟶ potential (V)

Pressure drop ⟶ voltage drop

Pump ⟶ generator

Topic 1- SCADA Introduction References

Antunes, Ricardo; Poshdar, Mani (2018). "Envision of an integrated information system for project-driven production in construction". Proc. 26th Annual Conference of the International. Group for Lean Construction (IGLC): 134–143. doi:10.24928/2018/0511. Retrieved 27 December 2018.

Boys, Walt (18 August 2009). "Back to Basics: SCADA". Automation TV: Control Global - Control Design.

"Cyberthreats, Vulnerabilities and Attacks on SCADA Networks" (PDF). Rosa Tang, berkeley.edu. Archived from the original (PDF) on 13 August 2012. Retrieved 1 August 2012.

Boyer, Stuart A. (2010). SCADA Supervisory Control and Data Acquisition. USA: ISA - International Society of Automation. p. 179. ISBN 978-1-936007-09-7.

Jeff Hieb (2008). Security Hardened Remote Terminal Units for SCADA Networks. University of Louisville.

Aquino-Santos, Raul (30 November 2010). Emerging Technologies in Wireless Ad-hoc Networks: Applications and Future Development: Applications and Future Development. IGI Global. pp. 43–. ISBN 978-1-60960-029-7.

"Introduction to Industrial Control Networks" (PDF). IEEE Communications Surveys and Tutorials. 2012.

Bergan, Christian (August 2011). "Demystifying Satellite for the Smart Grid: Four Common Misconceptions". Electric Light & Powers. Utility Automation & Engineering T&D. Tulsa, OK: PennWell. 16 (8). Four. Retrieved 2 May 2012. satellite is a cost-effective and secure solution that can provide backup communications and easily support core smart grid applications like SCADA, telemetry, AMI backhaul and distribution automation

OFFICE OF THE MANAGER NATIONAL COMMUNICATIONS SYSTEM October 2004. "Supervisory Control and Data Acquisition (SCADA) Systems" (PDF). NATIONAL COMMUNICATIONS SYSTEM.

J. Russel. "A Brief History of SCADA/EMS (2015)". Archived from the original on 11 August 2015.

Security Hardened Remote Terminal Units for SCADA Networks. ProQuest. 2008. pp. 12–. ISBN 978-0-549-54831-7.

"SCADA as a service approach for interoperability of micro-grid platforms". Sustainable Energy, Grids and Network. 2016. doi:10.1016/j.segan.2016.08.001.

"SCADA as a service approach for interoperability of micro-grid platforms", Sustainable Energy, Grids and Network, 2016, doi:10.1016/j.segan.2016.08.001

"ICSA-11-231-01—INDUCTIVE AUTOMATION IGNITION INFORMATION DISCLOSURE VULNERABILITY" (PDF). 19 Aug 2011. Retrieved 21 Jan 2013.

"ICSA-11-094-01—WONDERWARE INBATCH CLIENT ACTIVEX BUFFER OVERFLOW" (PDF). 13 Apr 2011. Retrieved 26 Mar 2013.

D. Maynor and R. Graham (2006). "SCADA Security and Terrorism: We're Not Crying Wolf" (PDF).

Robert Lemos (26 July 2006). "SCADA system makers pushed toward security". Security Focus. Retrieved 9 May 2007.

"Industrial Security Best Practices" (PDF). Rockwell Automation. Retrieved 26 Mar 2013.

Slay, J.; Miller, M. (November 2007). "Chpt 6: Lessons Learned from the Maroochy Water Breach". Critical infrastructure protection (Online-Ausg. ed.). Springer Boston. pp. 73–82. ISBN 978-0-387-75461-1. Retrieved 2 May 2012.

http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf

"Security for all". InTech. June 2008. Retrieved 2 May 2012.

Topic 1- SCADA Introduction Post Quiz

Answers are found behind the Glossary.

SCADA Acronyms and Abbreviations

Identify the following terms

1. FTP

2. HMI

3. ICS

4. LAN

True or False

5. A "historian", is a software service within the HMI which accumulates time-stamped data, events, and alarms in a database which can be queried or used to populate graphic trends in the HMI. True or False

6. The historian is a client that controls PLCs from a data acquisition server. True or False

7. PLCs are often used in place of RTUs as field devices because they are more economical, versatile, flexible and configurable. True or False

8. SCADA systems are crucial for industrial organizations since they help to maintain efficiency, process data for smarter decisions, and communicate system issues to help mitigate downtime. True or False

Fill-in-the Blank

9. The basic SCADA _____begins with programmable logic controllers (PLCs) or remote terminal units (RTUs). PLCs and RTUs are microcomputers that communicate with an array of objects such as factory machines, HMIs, sensors, and end devices, and then route the information from those objects to computers with SCADA software.

10. What missing term starts at the PLC or RTU level, which includes the equipment status reports, and meter readings?

11. SCADA systems are commonly used in alarm systems. The alarm has only two digital status points with values_____.

12. To alert the SCADA operators and managers, text messages and emails are sent along with_____.

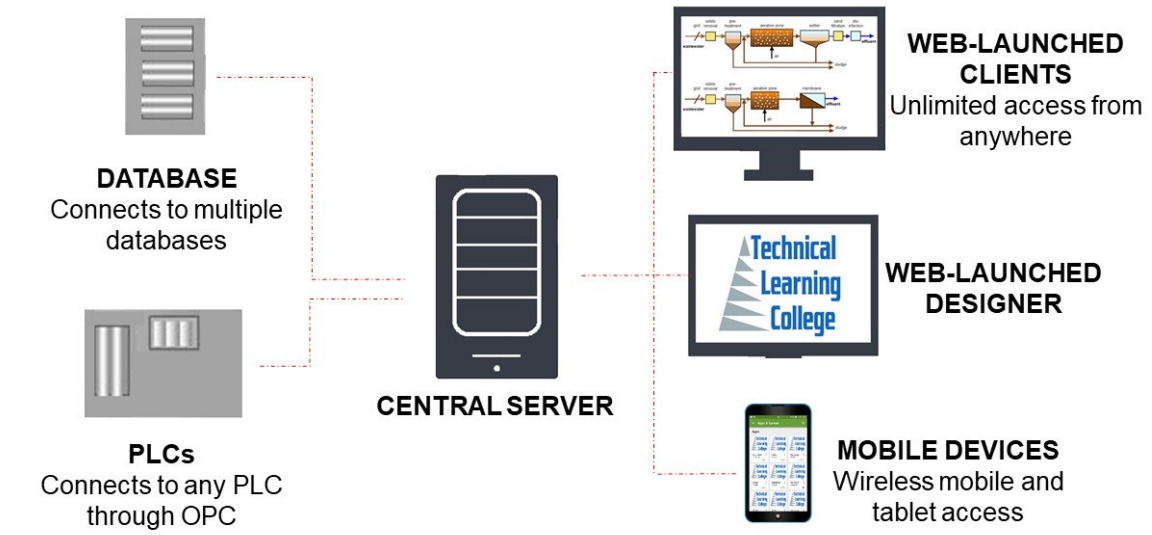
13. By converting and sending the electrical signals to the equipment, _____may control the equipment, like closing or opening a valve or a switch, or setting the speed of the pump.

14. For increasing the system integrity, multiple servers are occasionally configured in_____, providing monitoring and continuous control during server failures.

15. "Smart" RTUs, or standard PLCs, are capable of autonomously executing simple logic processes without involving the_____.

Topic 2 - SCADA, HMI, DCS, and PLCs Section

Topic 2 - Section Focus: You will learn the various SCADA components and their purposes in this section, including Human Machine Interface (HMI), Distributed Control System (DCS) and Programmable Logic Controllers (PLCs). You will be able to understand and describe the purposes of HMI, DCS, and PLCs. There is a post quiz at the end of this section to review your comprehension and a final examination in the Assignment for your contact hours.
Topic 2 – Scope/Background: SCADA systems are used to control dispersed assets where centralized data acquisition is as important as control. These systems are used in distribution systems such as water distribution and wastewater collection systems, oil and gas pipelines, electrical utility transmission and distribution systems, and rail and other public transportation systems.



MODERN SCADA DIAGRAM

SCADA, HMI, DCS, and PLCs Detailed Overview

SCADA systems are highly distributed systems used to control geographically dispersed assets, often scattered over thousands of square miles, 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 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.

Distributed Control System (DCSs) are used to control industrial processes such as electric power generation, oil and gas refineries, water and wastewater treatment, and chemical, food, and automotive production. DCSs are integrated as a control architecture containing a supervisory level of control overseeing multiple, integrated subsystems 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 programmable controllers (PLC) are employed in the field and proportional, integral, and/or differential settings on the PLC are tuned to provide the desired tolerance as well as the rate of self-correction during process upsets. DCSs 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 regulatory control of discrete processes such as automobile assembly lines and power plant soot blower controls. PLCs are used extensively in almost all industrial and water/wastewater treatment 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.

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.

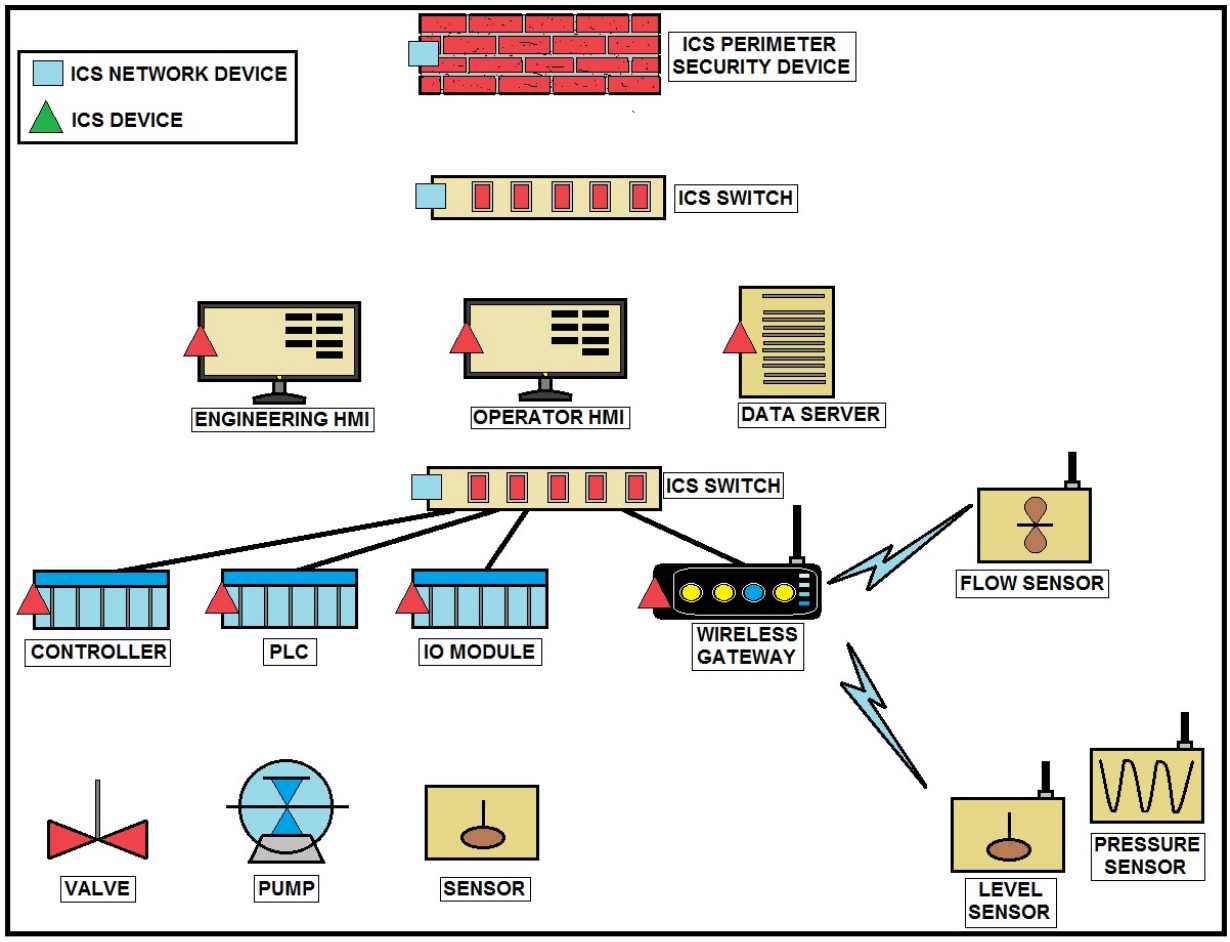
Both process-based and discrete-based industries utilize the same types of control systems, sensors, and networks. Some facilities are a hybrid of discrete and process-based manufacturing. While control systems used in distribution and manufacturing industries are very similar in operation, they are different in some aspects. One of the primary differences is that DCS or PLC-controlled subsystems 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 information technology (IT) security into these systems. Throughout the remainder of this document, SCADA systems, DCSs and PLC systems will be referred to as ICSs 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:



INDUSTRIAL CONTROL SYSTEM (ICS) EXAMPLE

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 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 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.

2.3 Key ICS Components - Quick Review
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 both SCADA systems, DCSs 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 is designed to communicate 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 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, drum 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 DCSs. 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 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 sensors communicate with the fieldbus controller using a specific protocol. 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.

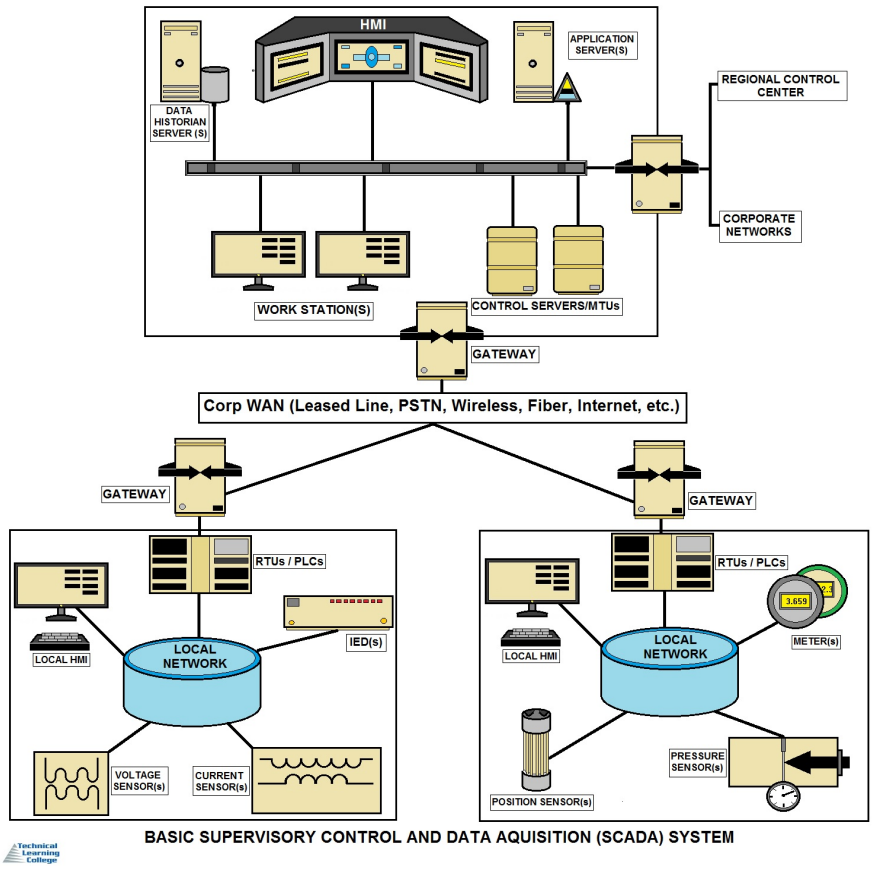
Firewall
A firewall protects devices on a network by monitoring and controlling communication packets using predefined filtering policies. Firewalls are also useful in managing ICS network segregation strategies.

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 both SCADA systems, DCSs and PLCs for gaining remote access for operational functions such as entering command 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 Detailed Overview

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 gas pipelines, electrical utility transmission and distribution systems, and rail and other public transportation systems.



BASIC SUPERVISORY CONTROL AND DATA AQUISITION (SCADA) SYSTEM

Figure 2-2 shows the components and general configuration of a SCADA system. The control center houses a control server (MTU) and the communications routers. Other control center components include the HMI, engineering workstations, and the data historian, which are all connected by a LAN. The control center collects and logs information gathered by the field sites, displays information to the HMI, and 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.

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 go outside acceptable values. An IED, such as a protective relay, may communicate directly to the SCADA master station, or a local RTU may poll the IEDs to collect the data and pass it to the SCADA master station.

IEDs provide a direct interface to control and monitor equipment and sensors. IEDs may be directly polled and controlled by the SCADA master station 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.

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 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.

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.

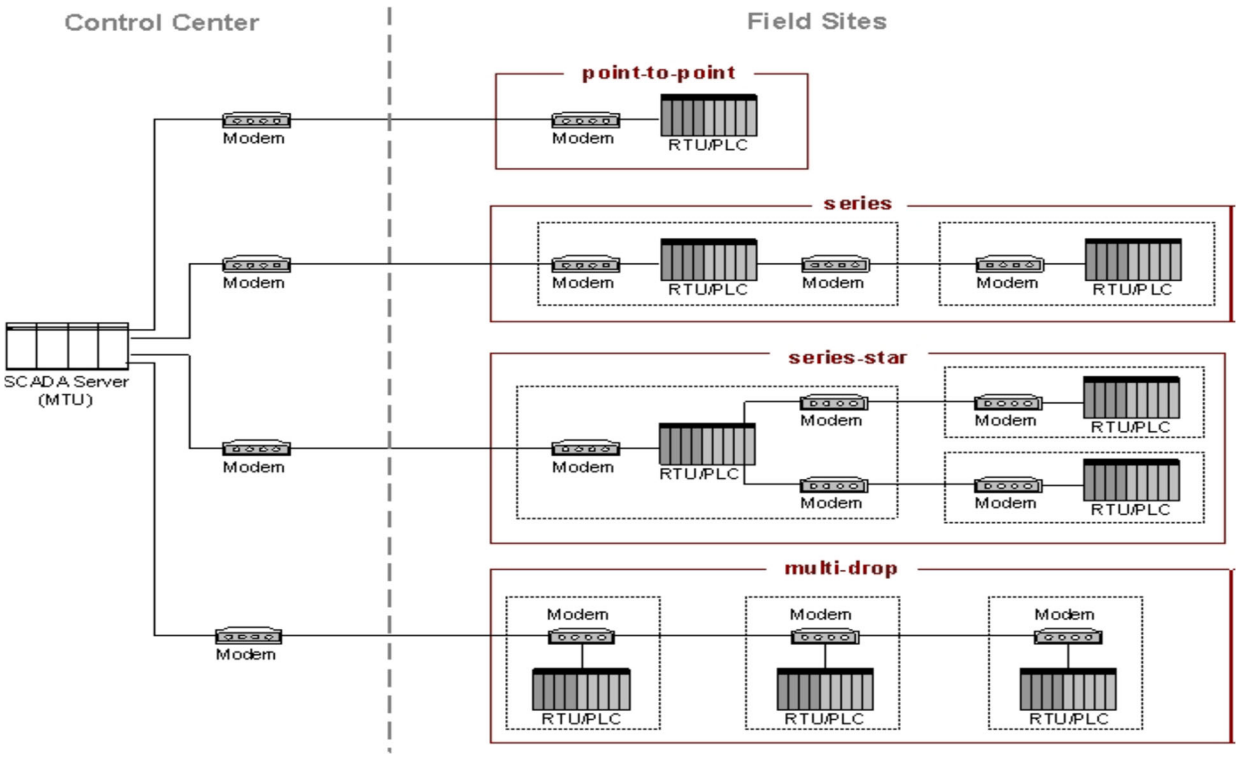


Figure 2-3. Basic SCADA Communication Topologies

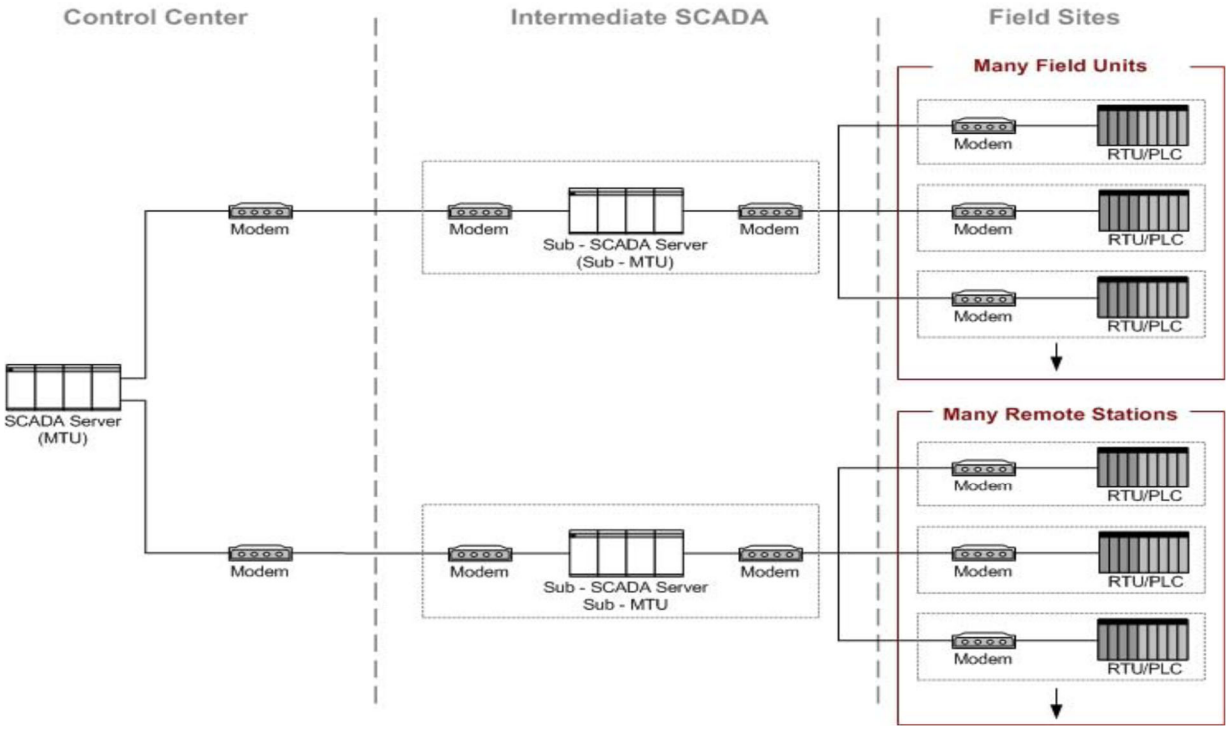


Figure 2-4. Large SCADA Communication Topology

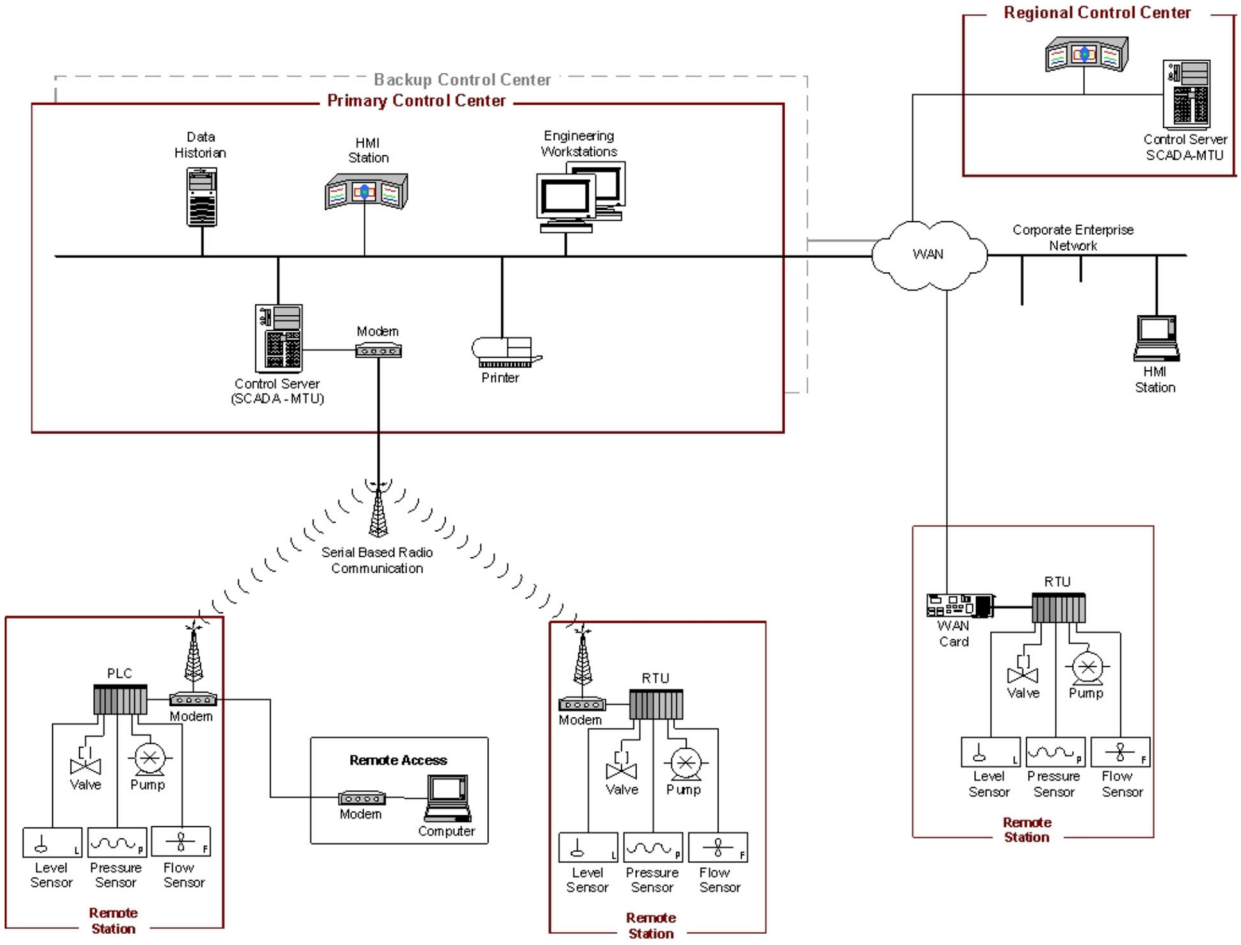


Figure 2-5. SCADA System Implementation Example
(Distribution Monitoring and Control)

Figure 2-5 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 sits 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, etc.) 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.

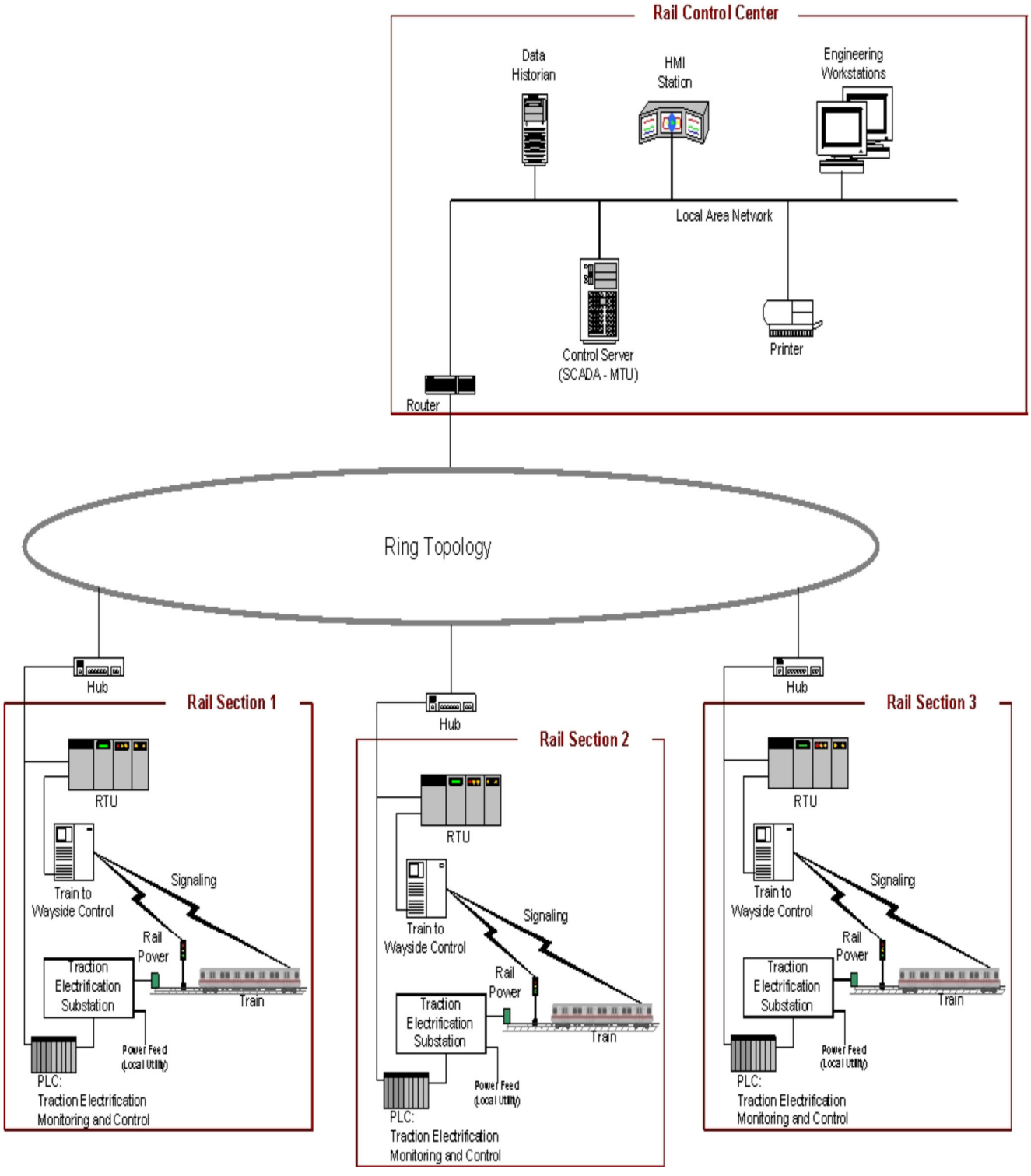


Figure 2-6. SCADA System Implementation Example (Rail Monitoring and Control)

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 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 based on condition monitoring).

2.5 Distributed Control Systems

DCSs are used to control production systems within the same geographic location for industries such as oil and gas 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 most 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.

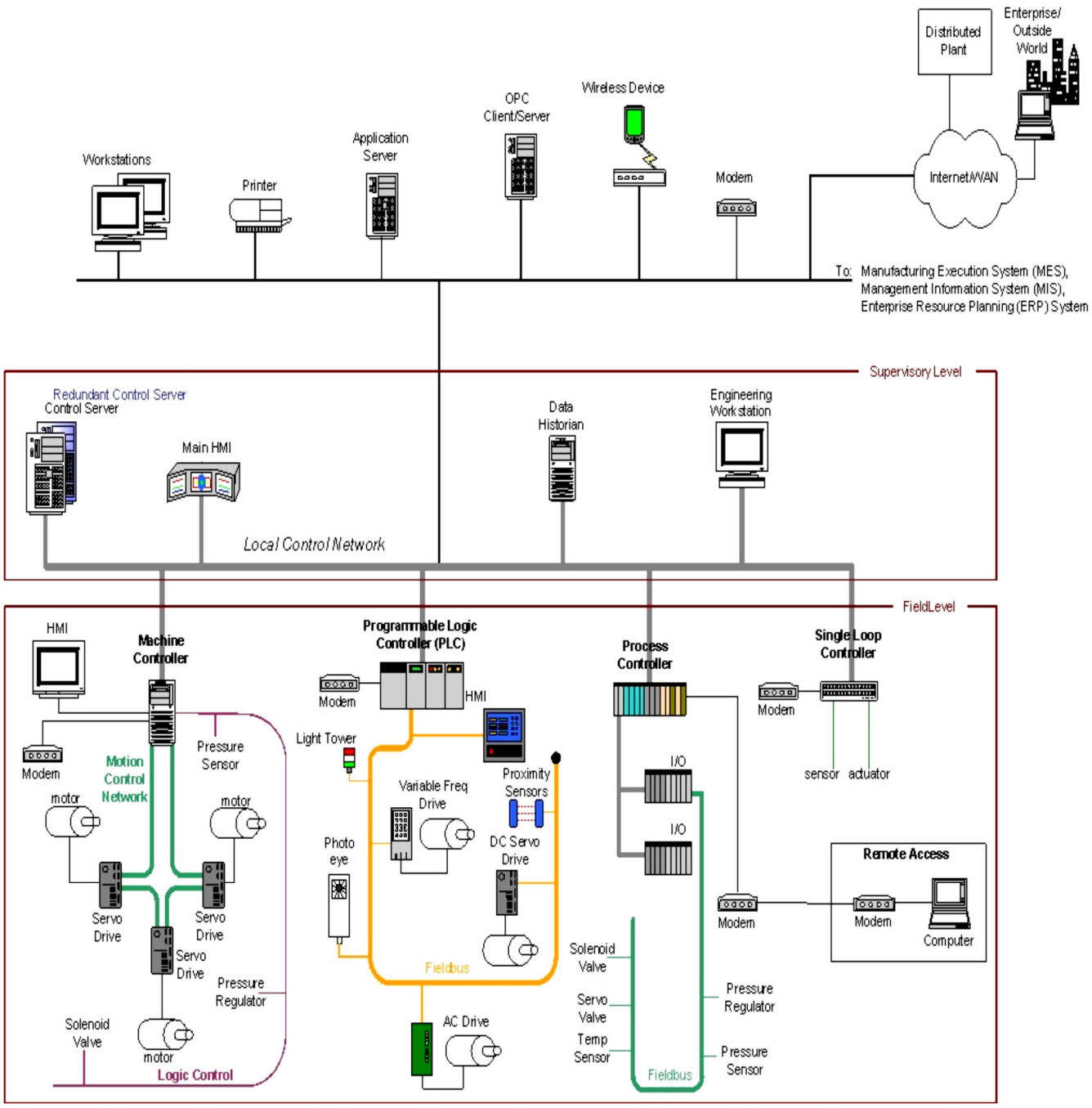


Figure 2-7. DCS Implementation Example

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.

2.6 Programmable Logic Controllers

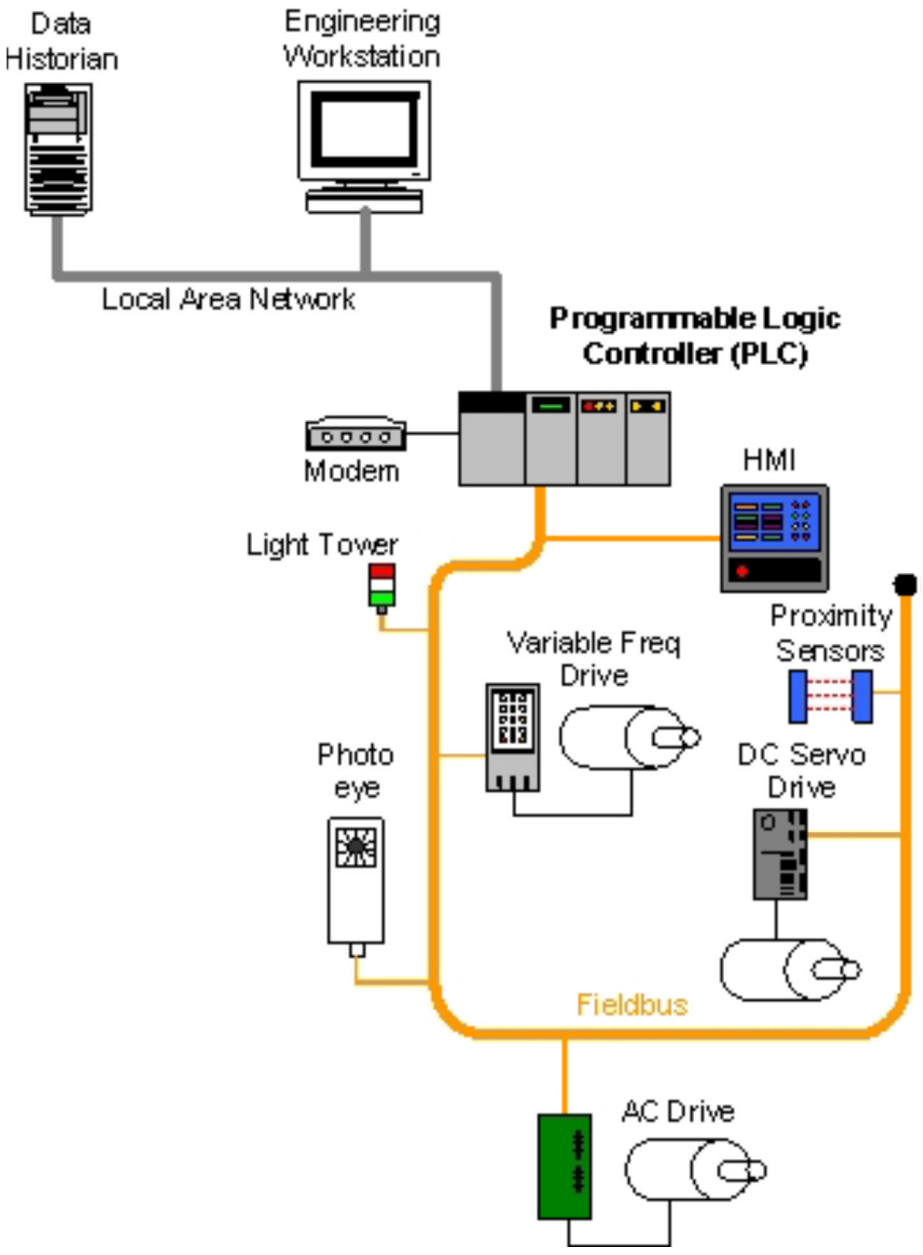


Figure 2-8. PLC Control System Implementation Example

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 DCSs, 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.

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 gas distribution, including pipelines, ships, trucks, and rail systems, as well as wastewater collection systems.

SCADA systems and DCSs are often tied 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 affect oil and natural gas production, refinery operations, water treatment systems, wastewater collection systems, and pipeline transport systems that rely on the grid for power.

Topic 2 - SCADA, HMI, DCS, and PLCs Section References

[1] Frazer, Roy, *Process Measurement and Control – Introduction to Sensors, Communication Adjustment, and Control*, Prentice-Hall, Inc., 2001.

[2] Falco, Joe, et al., *IT Security for Industrial Control Systems*, NIST IR 6859, 2003, http://www.isd.mel.nist.gov/documents/falco/ITSecurityProcess.pdf.

[3] Bailey, David, and Wright, Edwin, *Practical SCADA for Industry*, IDC Technologies, 2003.

[4] Boyer, Stuart, *SCADA Supervisory Control and Data Acquisition*, 2nd Edition, ISA, 1999.

[5] AGA-12, Cryptographic Protection of SCADA Communications, Part 1: Background, Policies and Test Plan, September, 2005, http://www.gtiservices.org/security/AGA12_part1_draft6.pdf.

[6] Erickson, Kelvin, and Hedrick, John, *Plant Wide Process Control*, Wiley & Sons, 1999.

[7] Berge, Jonas, *Fieldbuses for Process Control: Engineering, Operation, and Maintenance*, ISA, 2002.

Topic 2 - SCADA, HMI, DCS, and PLCs Section Post Quiz

Answers are found behind the Glossary
True or False

1. PLCs are integrated as a control architecture containing a supervisory level of control overseeing multiple, integrated subsystems that are responsible for controlling the details of a localized process. True or False

2. DCSs are computer-based solid-state devices that control industrial equipment and processes. True or False

3. 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. True or False

4. 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. True or False

5. Operators and engineers use RTUs to configure set points, control algorithms, and adjust and establish parameters in the controller. The RTUs also displays process status information and historical information. True or False

6. The control server hosts the DCS or PLC supervisory control software that is designed to communicate with lower-level control devices. The control server accesses subordinate control modules over an ICS network. True or False

7. RTUs are office devices often equipped with wireless radio interfaces to support remote situations where wire-based communications is available. Sometimes PLCs are implemented as office devices to serve as RTUs; in this case, the PLC is often referred to as an RTU. True or False

8. An IED is a “dumb” sensor/actuator containing no intelligence required to acquire data, communicate to other devices, and perform local processing and control.
True or False

9. The use of IEDs in SCADA and DCS systems allows for automatic control at the local level. True or False

Fill-in-the-Blank

10. The _____is a centralized database for logging all process information within an ICS.

11. The IO server is a control component responsible for collecting, buffering and providing access to process information from control sub-components such as_____.

12. _____can reside on the control server or on a separate computer platform.

13. Use of _____eliminates the need for point-to-point wiring between the controller and each device.

14. The_____ connects the supervisory control level to lower-level control modules.

15. _____are distinct devices, areas and locations of a control network for remotely configuring control systems and accessing process data.

Topic 3 - ICS Characteristics, Threats and Vulnerabilities

Topic 3 - Section Focus: You will learn the basics of the Industrial Control System (ICS) threat and vulnerabilities. At the end of this section, you will be able to understand and describe various components, technologies, threats and vulnerabilities related to ICSs and IT systems. There is a post quiz at the end of this section to review your comprehension and a final examination in the Assignment for your contact hours.

Topic 3 – Scope/Background: 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 ICSs must understand the link between safety and security.

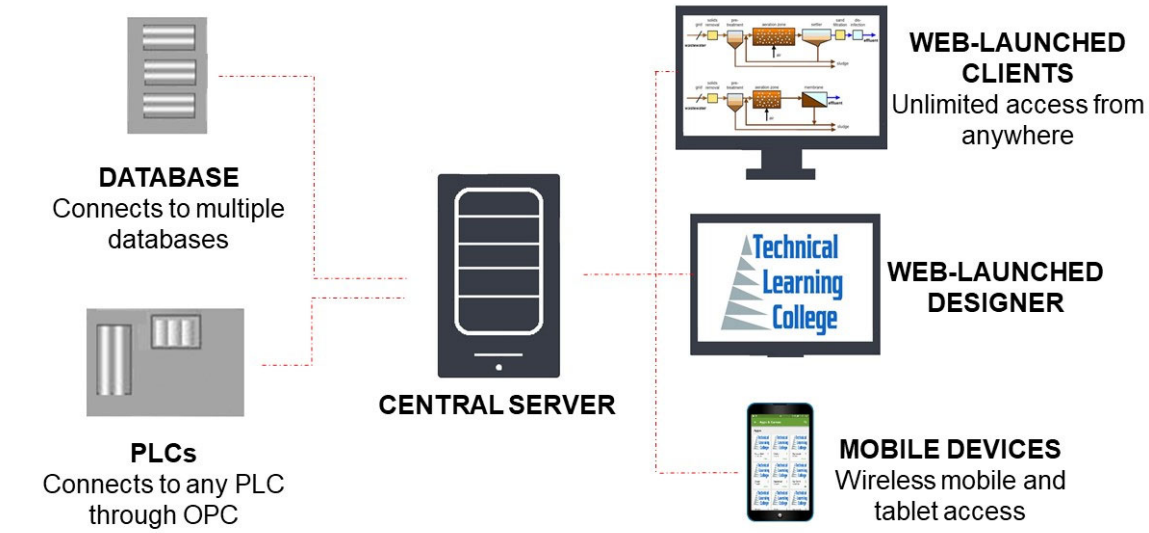
.

ICS Characteristics, Threats and Vulnerabilities

Most Industrial Control Systems (ICSs) 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 communications 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 ICSs exposed them to new types of threats and significantly increased the likelihood that ICSs could be compromised. This section describes the unique security characteristics of ICSs, the vulnerabilities in ICS implementations, and the threats and incidents that ICSs may face. Section 3.7 presents several examples of actual ICS cyber security incidents.



Technical Learning College

MODERN SCADA DIAGRAM

3.1 Comparing ICS and IT Systems

Initially, ICSs had little resemblance to IT systems in that ICSs 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 ICSs 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 ICSs 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.

ICSs have many characteristics that differ from traditional Internet-based information processing 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, negative impact to a nation's economy, and compromise of proprietary information. ICSs have different performance and reliability requirements and use operating systems and applications that may be considered unconventional to typical IT personnel. Furthermore, the goals of safety and efficiency can sometimes conflict with security in the design and operation of control systems (e.g., requiring password authentication and authorization should not hamper emergency actions for ICSs.) The following lists some special considerations when considering security for ICSs:

Performance Requirements
ICSs are generally time-critical; delay is not acceptable for the delivery of information, and high throughput is typically not essential. In contrast, IT systems typically require high throughput, but they can typically withstand substantial levels of delay and jitter. ICSs must exhibit deterministic responses.

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, use of typical IT strategies such as rebooting a component, are usually not acceptable due to the impact on the requirements for high availability, reliability and maintainability of the ICS.

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 ICSs must understand the 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 ICSs, edge clients (e.g., PLC, operator station, DCS controller) need to be carefully protected since they are directly responsible for controlling the end processes. The protection of the central server is still very important in an ICS, since the central server could possibly adversely impact every edge device.

Unintended Consequences
ICSs can have very complex interactions with physical processes and consequences in the ICS domain can manifest in physical events. All security functions integrated into the industrial control system must be tested 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 ICSs, automated response time or system response to human interaction is critical. For example, requiring password authentication and authorization on an HMI should not hamper emergency actions for industrial control systems. 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 applications are more difficult to upgrade in a control system network. Many systems may not have desired features including encryption capabilities, error logging, and password protection.

Resource Constraints
ICSs 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 agreements and loss of service support can occur if third party applications are installed.

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 systems represent 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 ICSs 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. Change management is also applicable to hardware and firmware. The change management process, when applied to ICSs, requires careful assessment by ICS experts working in conjunction with security and IT personnel.

Managed Support
Typical IT systems allow for diversified support styles, perhaps to support disparate but interconnected technology architectures. For ICSs, 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 3-5 years, with brevity due to the quick evolution of technology. For ICSs 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 15-20 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 ICSs.

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 maybe acceptable	Real-time Response is time-critical Modest throughput is acceptable High delay and/or jitter is a serious concern
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 Outages must be planned and scheduled days/weeks in advance High availability requires exhaustive pre-deployment testing
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 is not acceptable Major risk impact is regulatory non-compliance, 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 still important
Unintended Consequences	Security solutions are designed around typical IT systems	Security tools must be tested 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	Response to human and other emergency interaction is critical Access to ICS should be strictly controlled, yet not hamper 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 custom operating systems often without security capabilities 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, with minimal memory and computing resources to support the addition of security technology
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
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

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.

Available computing resources for ICSs (including central processing unit [CPU] time and memory) tend to be very limited because these systems were designed to maximize control system resources, with little to no extra capacity for third-party cyber security solutions.

Additionally, in some instances, third-party security solutions are not allowed due to vendor license 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. A cross-functional team of control engineers and IT 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 ICSs need to understand the reliability impacts of information security technologies before deployment. Some of the OSs and applications running on ICSs may not operate correctly with off-the-shelf IT 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 ICSs. Please note this list is in alphabetical order and not by greatest threat.

3.2.1 Potential ICS Vulnerabilities

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

Any given ICS will usually exhibit a subset of these vulnerabilities, but may also contain additional vulnerabilities unique to the particular ICS implementation that do not appear in this listing. Specific information on ICS vulnerabilities can be 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, 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.

Table 3-2. Adversarial Threats to ICSs

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.
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).

3.2.2 Platform Vulnerabilities

Vulnerabilities in ICSs 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.
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.
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 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 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 set to 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 unstaffed and may not be physically monitored.
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 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, 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.
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 little or no security capabilities.
Use of clear text	Many ICS protocols transmit messages in clear text across the transmission media, making them susceptible to eavesdropping by 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 ICS conferences (including “Black Hat” conferences) and available through technical papers and periodicals. Also, control system maintenance manuals are available from the vendors. This information can help adversaries to create successful attacks against ICSs.
Inadequate authentication and access control for configuration and programming software	Unauthorized access to configuration and programming software could provide the ability to corrupt 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 so security incidents may not be rapidly detected and countered.

3.3.1 Policy and Procedure Vulnerabilities

Vulnerabilities are often introduced into ICSs 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 ICSs. Table 3-3 describes potential policy and procedure vulnerabilities for ICSs.

Table 3-3. Policy and Procedure Vulnerabilities

Vulnerability	Description
Inadequate security policy for the ICS	Vulnerabilities are often introduced into ICSs due to inadequate policies or the lack of policies specifically for control system security.
No formal 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 best 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 no 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 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 should be held accountable for administering documented security policies and procedures.
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 as countermeasures 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 is needed 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.
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.

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.

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 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 IT security equipment	Using default configurations often leads to insecure and unnecessary open ports and exploitable network services running on hosts. Improperly configured firewall rules and router 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.
Control network services not within the control network	Where IT services such as DNS, 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
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 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.

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, FTP, and 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 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 ICSs 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. 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 technical field support personnel. Remote access 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 encryption have the increased risk of adversaries using these insecure connections to access remotely controlled systems. Without encryption to protect data as it flows through these insecure connections, and authentication mechanisms to limit access, there is little to protect the confidentiality and integrity of the information being transmitted. 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 human and plant safety.

Many of the interconnections between corporate networks and ICSs 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 networking resources 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 underlying 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. 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. 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 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, DCSs, or SCADA controllers, change alarm thresholds, or issue unauthorized commands to control equipment, which could potentially result in damage to equipment (if tolerances are exceeded), premature shutdown of processes (such as prematurely shutting down transmission lines), causing environmental incident, or even disabling of 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 unstaffed 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 and overloading the lines. This causes significant damage to transformers and other critical equipment, resulting in lengthy repair outages.
- A power plant serving a large metropolitan district has successfully isolated the control system from the corporate network of the plant, installed state-of-the-art firewalls, and implemented intrusion detection and prevention technology. An engineer innocently downloads information on a continuing education seminar at a local college, inadvertently introducing a virus into the control network. Just before the morning peak, the operator screens go blank and the system is shut down.

Although these scenarios are hypothetical, they represent the kinds of potential incident scenarios for an ICS. Section 3.7 provides summaries of several real 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 an Industrial Security Incident Database (ISID), which is designed to track incidents of a cyber security nature that directly affect ICSs 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.

There are three broad categories of control system incidents:

- Intentional targeted attacks such as gaining unauthorized access to files, performing a DoS, or spoofing e-mails (i.e., forging the sender's identity for an e-mail)
- Unintentional consequences or collateral damage from worms, viruses or control system failures
- Unintentional internal security consequences, such as inappropriate testing of operational systems or unauthorized system configuration changes.

Of the three, targeted attacks are the least frequent. Targeted attacks are potentially the most damaging, but also require detailed knowledge of the system and supporting infrastructure. Therefore, the most likely threat agent is the unintentional threat or a disgruntled employee, former employee, or someone else who has worked with or for the organization [12].

3.7 Unintentional Consequences

CSX Train Signaling System
In August 2003, the Sobig computer virus was blamed for shutting down train signaling systems throughout the east coast of the U.S. The virus infected the computer system at CSX Corp.'s Jacksonville, Florida headquarters, shutting down signaling, dispatching, and other systems. According to Amtrak spokesman Dan Stessel, ten Amtrak trains were affected in the morning. Trains between Pittsburgh and Florence, South Carolina were halted because of dark signals, and one regional Amtrak train from Richmond, Virginia to Washington and New York was delayed for more than two hours. Long-distance trains were delayed between four and six hours.

Davis-Besse
In August 2003, the Nuclear Regulatory Commission confirmed that in January 2003, the Microsoft SQL Server worm known as Slammer infected a private computer network at the idled Davis-Besse nuclear power plant in Oak Harbor, Ohio, disabling a safety monitoring system for nearly five hours. In addition, the plant's process computer failed, and it took about six hours for it to become available again. Slammer reportedly also affected communications on the control networks of at least five other utilities by propagating so quickly that control system traffic was blocked.

Northeast Power Blackout
In August 2003, failure of the alarm processor in First Energy's SCADA system prevented control room operators from having adequate *situational awareness* of critical operational changes to the electrical grid. Additionally, effective reliability oversight was prevented when the state estimator at the Midwest Independent System Operator failed due to incomplete information on topology changes, preventing contingency analysis. Several key 345kV transmission lines in Northern Ohio trip due to contact with trees. This eventually initiates cascading overloads of additional 345 kV and 138 kV lines, leading to an uncontrolled cascading failure of the grid. 61,800 MW load is lost as 508 generating units at 265 power plants trip.

Zotob Worm
In August 2005, a round of Internet worm infections knocked 13 of DaimlerChrysler's U.S. automobile manufacturing plants offline for almost an hour; stranding workers as infected Microsoft Windows systems were patched. Plants in Illinois, Indiana, Wisconsin, Ohio, Delaware, and Michigan were knocked offline. While the worm affected primarily Windows 2000 systems, it also affected some early versions of Windows XP. Symptoms include the repeated shutdown and rebooting of a computer. Zotob and its variations caused computer outages at heavy-equipment maker Caterpillar Inc., aircraft-maker Boeing, and several large U.S. news organizations.

Taum Sauk Water Storage Dam Failure
In December 2005, the Taum Sauk Water Storage Dam suffered a catastrophic failure releasing a billion gallons of water. The failure of the reservoir occurred as the reservoir was being filled to capacity or may have possibly been overtopped. The current working theory is that the reservoir's berm was overtopped when the routine nightly pump-back operation failed to cease when the reservoir was filled. According to AmerenUE, the gauges at the dam read differently than the gauges at the Osage plant at the Lake of the Ozarks, which monitors and operates the Taum Sauk plant remotely. The stations are linked together using a network of microwave towers, and there are no operators on-site at Taum Sauk.

Unintentional Internal Security Consequences

Vulnerability Scanner Incidents
While a ping sweep was being performed on an active SCADA network that controlled 9-foot robotic arms, it was noticed that one arm became active and swung around 180 degrees. The controller for the arm was in standby mode before the ping sweep was initiated. In a separate incident, a ping sweep was being performed on an ICS network to identify all hosts that were attached to the network, for inventory purposes, and it caused a system controlling the creation of integrated circuits in the fabrication plant to hang. This test resulted in the destruction of $50,000 worth of wafers. Refer to Section 4.2.6 for additional guidance on ICS vulnerability assessments.

Penetration Testing Incident
A gas utility hired an IT security consulting organization to conduct penetration testing on its corporate IT network. The consulting organization carelessly ventured into a part of the network that was directly connected to the SCADA system. The penetration test locked up the SCADA system and the utility was not able to send gas through its pipelines for four hours. The outcome was the loss of service to its customer base for those four hours.

Bellingham, Washington Gasoline Pipeline Failure
In June 1999, 237,000 gallons of gasoline leaked from a 16” pipeline and ignited 1.5 hours later causing 3 deaths, 8 injuries, and extensive property damage. The pipeline failure was exacerbated by control systems not able to perform control and monitoring functions. “Immediately prior to and during the incident, the SCADA system exhibited poor performance that inhibited the pipeline controllers from seeing and reacting to the development of an abnormal pipeline operation.” A key recommendation from the NTSB report issued October 2002 was to utilize an off-line development system for implementing and testing changes to the SCADA database.

Maroochy Shire Sewage Spill
The Maroochydore District Court heard that 49-year-old Vitek Boden had conducted a series of electronic attacks on the Maroochy Shire sewage control system after a job application he had made was rejected by the area's Council. At the time he was employed by the company that had installed the system. Boden made at least 46 attempts to take control of the sewage system during March and April 2000. On 23 April, the date of Boden's last hacking attempt, police who pulled over his car found radio and computer equipment. Marine life died, the creek water turned black and the stench was unbearable for residents.

Topic 3 - ICS Characteristics, Threats and Vulnerabilities Section References

[7] Berge, Jonas, *Fieldbuses for Process Control: Engineering, Operation, and Maintenance*, ISA, 2002.

[8] Peerenboom, James, *Infrastructure Interdependencies: Overview of Concepts and Terminology*, Argonne National Laboratory, http://www.pnwer.org/pris/peerenboom_pdf.pdf.

[9] Rinaldi, et al., *Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies*, IEEE Control Systems Magazine, 2001, http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf.

[10] GAO-04-354, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*, U.S. GAO, 2004, http://www.gao.gov/new.items/d04354.pdf.

[11] Weiss, Joseph, "Current Status of Cyber Security of Control Systems", Presentation to Georgia Tech Protective Relay Conference, May 8, 2003.

[12] Keeney, Michelle et al., *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*, United States Secret Service and Carnegie Mellon Software Institute, 2005, http://www.cert.org/archive/pdf/insidercross051105.pdf.

Topic 3 - ICS Characteristics, Threats and Vulnerabilities Post Quiz

True or False

1. Initially, ICSs resembled IT systems in that the two were the same thing.
True or False

2. In some cases, new security solutions are needed that are tailored to the ICS environment. True or False

3. ICSs are generally not time-critical; delay is acceptable for the delivery of information, and high throughput is typically not essential. True or False

4. In a typical IT system, data confidentiality and integrity are typically the primary concerns. True or False

5. 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.
True or False

Fill-in-the-Blank

6. In a typical IT system, _____can be implemented without significant regard for data flow.

7. Software and hardware applications are more difficult to _____in a control system network.

8. _____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.

9. Typical IT components have a lifetime on the order of _____years, with brevity due to the quick evolution of technology.

10. For ICSs 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 _____years and sometimes longer.

11. To protect against adversarial threats (as well as known natural threats), it is necessary to create a _____for the ICS.

12. _____ in ICSs can occur due to flaws, misconfigurations, or poor maintenance of their platforms, including hardware, operating systems, and ICS applications.

13. Security documentation, along with management support, is the _____ of any security program.

14. The demand for remote access has encouraged many organizations to establish _____that enable ICS engineers and support personnel to monitor and control the system from points outside the control network.

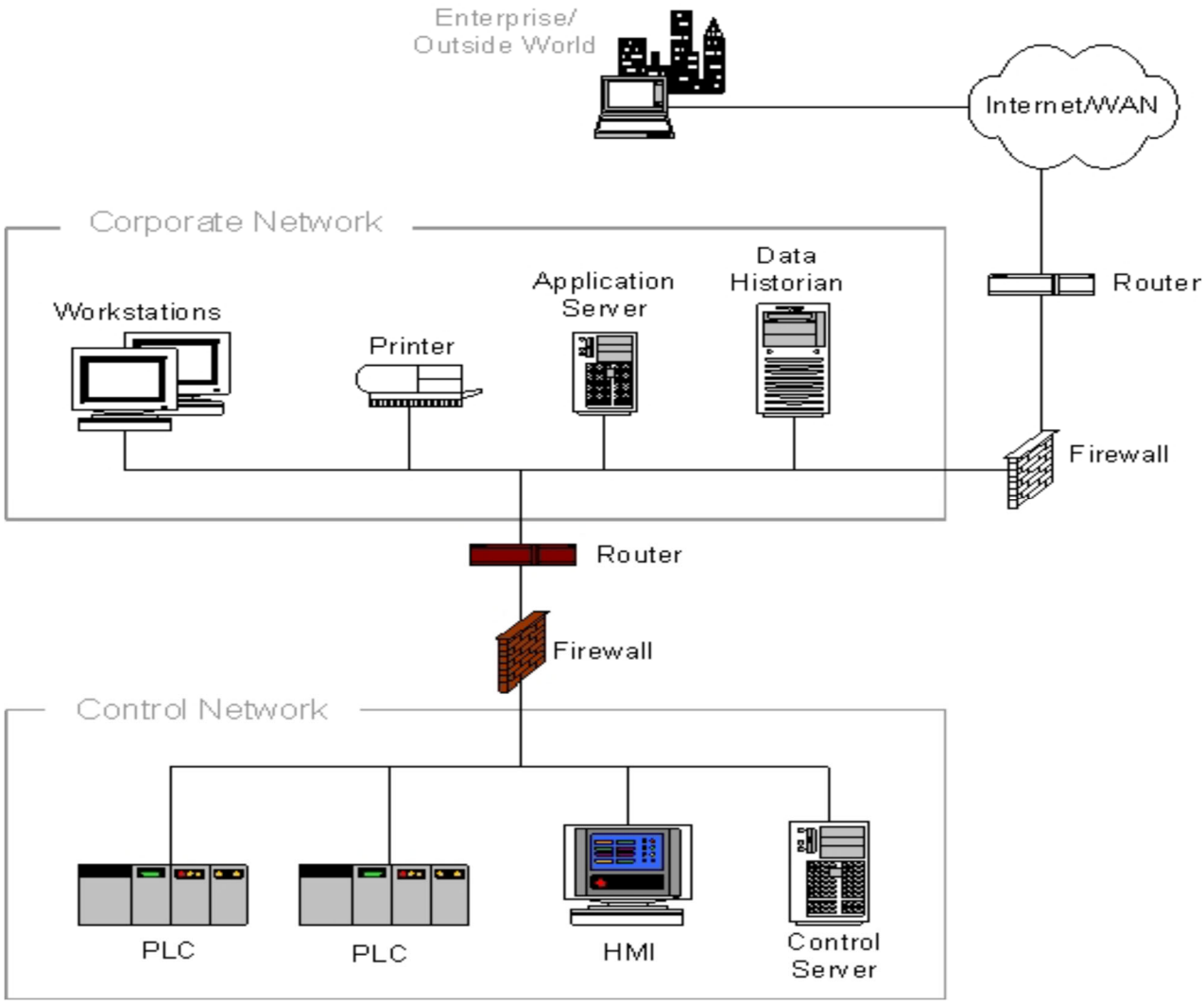
15. Unless appropriate security controls are deployed, vulnerabilities can expose all levels of the ICS network architecture to complexity-induced error, adversaries and a variety of cyber threats, including_____.

Topic 4- ICS Security Program Development Section

4. ICS Security Program Development and Deployment

Topic 4 - Section Focus: You will learn the basics securing an Industrial Control System (ICS) and security threats to the SCADA system. At the end of this section, you will be able to understand and describe various methods of protecting the ICS system from attacks. There is a post quiz at the end of this section to review your comprehension and a final examination in the Assignment for your contact hours.

Topic 4 – Scope/Background: The importance of secure systems should be further emphasized as business reliance on interconnectivity increases. DoS attacks and malware (e.g., worms, viruses) have become all too common and have already affected ICSs. In addition, a cyber breach in some sectors can have significant physical impacts



Firewall and Router between Corporate Network and Control Network

As described in Section 3.1, there are critical operational differences between ICS and IT systems that influence how specific security controls should be applied to the ICS.

Accordingly, organizations should develop and deploy an ICS security program.[14] ICS security plans and programs should be consistent with and integrated with existing IT security experience, programs, and practices, but must be tailored to the specific requirements and characteristics of ICS technologies and environments. Organizations should review and update their ICS security plans and programs regularly to reflect changes in technologies, operations, standards, and regulations, as well as the security needs of specific facilities.[15]

This section provides an overview of the development and deployment of an ICS security program. Section 4.1 describes how to establish a business case for an ICS security program, including suggested content for the business case. Section 4.2 discusses the development of a comprehensive ICS security program and provides information on several major steps in deploying the program. Information on specific security controls that might be implemented as part of the security program is given in Sections 5 and 6 of the document.

4.1 Business Case for Security

The first step to implementing a cyber-security program for ICS is to develop a compelling business case for the unique needs of the organization. The business case should capture the business concerns of senior management while being founded in the experience of those who are already dealing with many of the same risks. The business case provides the business impact and financial justification for creating an integrated cyber security program. It should include detailed information about the following:

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

Before presenting the business case to management, there should be a well-thought-out and developed security implementation plan. For example, simply requesting a firewall is insufficient for numerous reasons.

4.1.1 Benefits

Responsible risk management mandates that the threat to the ICS should be measured and monitored to protect the interests of employees, the public, shareholders, customers, vendors, and the larger society. Risk analysis enables costs and benefits to be weighed so that informed decisions can be made on also helps organizations by:

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

A strong safety and cyber security management program is fundamental to a sustainable business model.

4.1.2 Potential Consequences

The importance of secure systems should be further emphasized as business reliance on interconnectivity increases. DoS attacks and malware (e.g., worms, viruses) have become all too common and have already impacted ICSs. In addition, a cyber breach in some sectors can have significant physical impacts.

The major categories of impacts are as follows:

Physical Impacts. Physical impacts encompass the set of direct consequences of ICS failure. The potential effects of paramount importance include personal injury and loss of life. Other effects include the loss of property (including data) and damage to the environment.

Economic Impacts. Economic impacts are a second-order effect from physical impacts ensuing from an ICS incident. Physical impacts could result in repercussions to system operations, which in turn inflict a greater economic loss on the facility or organization. On a larger scale, these effects could negatively impact the local, regional, national, or possibly global economy.

Social Impacts. Another second-order effect, the consequence from the loss of national or public confidence in an organization, is many times overlooked. It is, however, a very real target and one that could be accomplished through an ICS incident.

A list of potential consequences of an ICS incident [29] is listed below. Note that items in this list are not independent.

In fact, one can lead to another. For example, release of hazardous material can lead to injury or death.

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

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

4.1.3 Key Components of the Business Case

There are four key components of the business case: prioritized threats, prioritized business consequences, prioritized business benefits, and estimated annual business impact.

4.1.3.1 Prioritized Threats

The list of potential threats provided in Section 3.2 needs to be refined to those threats that the organization believes could reasonably influence the facility to be secured. For instance, a food and beverage organization might not find terrorism a credible threat but might be more concerned with viruses, worms, and disgruntled employees.

4.1.3.2 Prioritized Business Consequences

The list of potential business consequences provided in Section 4.1.2 needs to be distilled to the particular business consequences that senior management will find the most compelling. For instance, a food and beverage organization that handles no toxic or flammable materials and typically processes its product at relatively low temperatures and pressures might not be concerned about equipment damage or environmental impact, but might be more concerned about loss of production availability and degradation of product quality. Regulatory compliance might also be a concern. Individuals should not minimize the potential consequences to avoid taking proper security risk mitigation actions.

The Sarbanes-Oxley Act requires corporate leaders to sign off on compliance with information accuracy and protection of corporate information. [16] Also, the demonstration of due diligence is required by most internal and external audit firms to satisfy shareholders and other organization stakeholders. By implementing a comprehensive cyber security program, management is exercising due diligence.

4.1.3.3 Prioritized Business Benefits

Improved control systems security and control system specific security policies can potentially improve control system reliability and availability. This also includes minimizing unintentional control system cyber security impacts from inappropriate testing, policies, and misconfigured systems.

4.1.3.4 Estimated Annual Business Impact

The highest priority items shown in the list of prioritized business consequences should be scrutinized to obtain an estimate of the annual business impact, preferably but not necessarily in financial terms. For the food and beverage organization example, the organization may have experienced a virus incident within its internal network that the information security staff estimated as resulting in a specific financial cost. Since the internal network and the control network are interconnected, it is conceivable that a virus originating from the control network could cause the same amount of business impact. NIST SP 800-30 [19] and ISO 17799 provide additional guidance on business impact.

4.1.4 Resources for Building Business Case

The main resources for information to help form a business case are external resources in trade and standards organizations, consulting firms and internal resources in related risk management programs or engineering and operations. External resources in trade and standards organizations can often provide useful tips as to what factors most strongly influenced their management to support their efforts and what resources within their organizations proved most helpful.

For different industries, these factors may be different, but there may be similarities in the roles that other risk management specialists can play. Appendix C provides a list and short description of some of the current activities in ICS security.

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

These resources can also provide insight into which managers are focused on dealing with which risks and, thus, which managers might be the most appropriate or receptive to serving as a champion. Internal resources in control systems engineering and operations can provide insight into the details of how control systems are deployed within the organization, such as the following:

- How networks are typically segregated
- What remote access connections are generally employed
- How high-risk combustion systems or safety instrumented systems are typically designed
- What security countermeasures are commonly used

4.1.5 Presenting the Business Case to Leadership

The business leadership will be responsible for approving and driving cyber security policies, assigning security roles, and implementing the cyber security program across the organization. Funding for the entire program can usually be done in phases. While some funding may be required to start the cyber security activity, additional funding can be obtained later as the security vulnerabilities and needs of the program are better understood and additional strategies are developed. Additionally, the costs (both direct and indirect) should be considered for retrofitting the ICS for security vs. addressing security to begin with.

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

4.2 Developing a Comprehensive Security Program

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

This section describes the basic process for developing a security program, including the following:
1. Obtain senior management buy-in
2. Build and train a cross-functional team
3. Define charter and scope
4. Define specific ICS policies and procedures
5. Define and inventory ICS assets
6. Perform a risk and vulnerability assessment
7. Define the mitigation controls
8. Provide training and raise security awareness for ICS staff.

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

The commitment to a security program begins at the top. Senior management must demonstrate a clear commitment to cyber security. Cyber security is a business responsibility shared by all members of the enterprise and especially by leading members of the business, process, and management teams.

Cyber security programs with visible, top-level support from organization leaders are more likely to achieve compliance, function more smoothly, and have earlier success than programs that do not have that support.

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

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

4.2.1 Senior Management Buy-in

It is critical for the success of the ICS security program that senior management [30] buy into and participate in the ICS security program. Senior management needs to be at a level that encompasses both IT and ICS operations.

4.2.2 Build and Train a Cross-Functional Team

It is essential for a cross-functional cyber security team to share their varied domain knowledge and experience to evaluate and mitigate risk in the ICS. At a minimum, the cyber security team should consist of a member of the organization's IT staff, a control engineer, security subject matter experts, and a member of the management staff.

Security knowledge and skills should include network architecture and design, security processes and practices, and secure infrastructure design and operation.

For continuity and completeness, the cyber security team should also include the control system vendor(s). The cyber security team should report directly to site management or the company's CIO/CSO, who in turn, accepts complete responsibility and accountability for the cyber security of the corporate and ICS networks. Management level accountability will help ensure an ongoing commitment to cyber security efforts.

While the control engineers will play a large role in securing the ICS, they will not be able to do so without collaboration and support from both the IT department and management. IT often has years of security experience, much of which is applicable to ICS. As the cultures of control engineering and IT are often significantly different and unknown to the other party, significant cross-cultural understanding and integration will be essential for the development of a collaborative security design and operation.

4.2.3 Define Charter and Scope

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

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

There may already be a program in place or being developed for the organization's IT business systems. The team should identify which existing practices to leverage and which practices are specific to the control system. In the long run, it will be easier to get positive results if the team can share resources with others in the organization that have similar objectives.

4.2.4 Define Specific ICS Policies and Procedures

Policies and procedures are at the root of every successful security program and wherever possible, ICS specific polices and procedures should be integrated with existing operational/management policies. The more transparent these policies are with all other procedures, the more likely they will be implemented at all levels. Policies and procedures help to ensure that security protection is both consistent and current to protect against evolving threats, and also help to educate. After the risks for the various systems are clearly understood, the cyber security team should examine existing security policies to see if they adequately address the risks to the ICS.

If needed, existing policies should be revised or new policies created to address desktop and business systems as well as the ICS. Few organizations have the resources to harden the ICS against all possible threats; management should guide the development of the security policies that will set the security priorities and goals for the organization so that the risks posed by the threats are mitigated sufficiently. Procedures that support the policies need to be developed so that the policies are implemented fully and properly for the ICS. Security procedures should be documented, tested, and updated periodically in response to policy and technology changes. Consider developing ICS security policies and procedures based on the Homeland Security Advisory System Threat Level, deploying increasingly heightened security postures as the Threat Level increases.

4.2.5 Define and Inventory ICS Systems and Networks Assets

The cyber security team should identify the applications and computer systems within the ICS, as well as the networks within and interfacing to the ICS. The focus should be on systems rather than just devices, and should include PLCs, DCSs, SCADA, and instrument-based systems that use a monitoring device such as an HMI. Assets that use a routable protocol or are dial-up accessible should be documented. As the team identifies the ICS assets, the information should be recorded in a standard format. The team should review and update the ICS asset list annually.

There are several commercial enterprise inventory tools that can identify and document all hardware and software resident on a network. Care must be taken before using these tools to identify ICS assets; teams should first conduct an assessment of how these tools work and what impact they might have on the connected control equipment.

Tool evaluation may include testing in similar, non-production control system environments to ensure that the tools do not adversely impact the production systems. Impact could be due to the nature of the information or the volume of network traffic. While this impact may be acceptable in IT systems, it is not acceptable in an ICS. Additional information and guidance on scanning and inventory tools is provided in Section 4.2.6.

4.2.6 Perform Risk and Vulnerability Assessment

Because every organization has a limited set of resources, organizations should perform a risk assessment for the ICS systems and use its results to prioritize the ICS systems based on the potential impact to each system. The organization should then perform a detailed vulnerability assessment for the highest-priority systems and assessments for lower-priority systems as deemed prudent/as resources allow. The vulnerability assessment will help identify any weaknesses that may be present in the systems that could allow the confidentiality, integrity, or availability of systems and data to be adversely affected, along with the related cyber security risks and mitigation approaches to reduce the risks.

Because of the potential for disruption to the devices, vulnerability scanners should be used with caution on production ICS networks [31]. A major concern is an accidental DoS to devices and networks. Vulnerability scanners often attempt to verify vulnerabilities by extensively probing and conducting a representative set of attacks against devices and networks. ICSs were designed and built to control and automate real-world processes or equipment. Given the wrong instructions, they could perform incorrect actions, causing waste, equipment damage, injury, or even deaths.

The following examples [32] demonstrate the danger:

- While a ping sweep was being performed on an active SCADA network that controlled 9-foot robotic arms, it was noticed that one arm became active and swung around 180 degrees. The controller for the arm was in standby mode before the ping sweep was initiated.
- On an ICS network, a ping sweep was being performed to identify all hosts that were attached to the network, for inventory purposes, and it caused a system controlling the creation of integrated circuits in the fabrication plant to hang. This test resulted in the destruction of $50,000 worth of wafers.
- A gas utility hired an IT security consulting organization to conduct penetration testing on its corporate IT network. The consulting organization carelessly ventured into a part of the network that was directly connected to the SCADA system. The penetration test locked up the SCADA system and the utility was not able to send gas through its pipelines for four hours. The outcome was the loss of service to its customer base for those four hours.

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

When performing an inventory or vulnerability scan on a system or network segment, there are several steps that are generally performed. Each step is listed in Table 4-1, along with the usual IT action and alternate suggested actions that should be taken instead for an ICS, making the outcomes of any testing safer. These techniques may make the work somewhat more difficult, but should help to mitigate problems associated with active scanning.

Table 4-1. Suggested Actions for ICS Vulnerability Assessments

To Be Identified	Usual IT Action	Suggested ICS Actions
Hosts, nodes, and networks	Ping sweep (e.g., nmap)	• Examine router configuration files or route tables • Perform physical verification (chasing wires) • Conduct passive network listening or use intrusion detection (e.g., snort) on the network • Specify a subset of IP addresses to be programmatically scanned
Services	Port scan (e.g., nmap)	• Do local port verification (e.g., netstat) • Scan a duplicate, development, or test system on a non- production network
Vulnerabilities within a service	Vulnerability scan (e.g., nessus)	• Perform local banner grabbing with version lookup in Common Vulnerabilities and Exposures (CVE) • Scan a duplicate, development, or test system on a non- production network

The commonality among the suggested ICS actions is that they do not generate traffic on production operational networks or against production systems. These less intrusive methods can gather most, if not all, of the same information as more active methods, without the risk of causing a failure by testing. Another factor to consider when choosing ICS testing methods is that these systems have little spare capacity as compared to IT systems. ICS systems have much greater longevity than their IT counterparts have, so their hardware is often well behind the state-of-the-art and can be easily overtaxed. In addition, ICS systems usually run at slow speeds on legacy networks that can be overwhelmed by the volume of traffic generated during active testing.

When any assessment of an ICS is being performed, ICS personnel must be aware that testing is occurring, and be prepared to immediately address any problems that arise. If manual control of the system is possible, personnel capable of performing manual control should be present during the security testing. Additionally, security auditors need to understand the ICS under test, the risk involved with the test, and the consequences associated with unintentional stimulus or DoS to the ICS.

4.2.7 Define the Mitigation Controls

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

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

Organizations should document and communicate the selected controls, along with the procedures for using the controls. As the team identifies mitigation strategies, risks may be identified that can be mitigated by “quick fix” solutions—low-cost, high-value practices that can significantly reduce risk. Examples of these solutions are restricting Internet access and eliminating e-mail access on operator control stations. Organizations should identify, evaluate, and implement suitable quick fix solutions as soon as possible to reduce security risks and achieve rapid benefits.

The Department of Energy (DOE) has a “21 Steps to Improve Cyber Security of SCADA Networks” [33] document that could be used as a starting point to outline specific actions to increase the security of SCADA systems and other ICSs.

4.2.8 Provide Training and Raise Security Awareness

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

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

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

Topic 4- ICS Security Program Development Section References

F-2 GUIDE TO SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) AND INDUSTRIAL CONTROL SYSTEMS SECURITY

[23] Barker, William, NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*, 2003, http://csrc.nist.gov/publications/nistpubs/800-59/SP800-59.pdf.

[24] Barker, William, NIST SP 800-60 Version 2.0, *Guide for Mapping Types of Information and Information systems to Security Categories*, 2004, http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V1-final.pdf.

[25] Souppaya, Murugiah, et al., NIST SP 800-70, *Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers*, 2005, http://csrc.nist.gov/checklists/docs/SP_800-70_20050526.pdf.

[26] Bowen, Pauline, et al., NIST SP 800-100, *Information Security Handbook: A Guide for Managers*, 2006, http://csrc.nist.gov/publications/drafts.html#sp800-100.

[27] *TR99.00.02: Integrating Electronic Security into the Manufacturing and Control Systems Environment*, ISA, 2004.

[28] NIST Security Configurations Checklists Program for IT Products, http://checklists.nist.gov/

[29] Stamp, Jason, et al., *Common Vulnerabilities in Critical Infrastructure Control Systems*, Sandia National Laboratories, 2003, http://www.sandia.gov/iorta/docs/SAND2003-1772C_Common_Vulnerabilities_CI_Control1.pdf.

[30] *SCADA Security - Advice for CEOs*, IT Security Expert Advisory Group (ITSEAG), http://www.ag.gov.au/agd/WWW/rwpattach.nsf/VAP/(930C12A9101F61D43493D44C70E84EAA)~SCADA+Security.pdf/$file/SCADA+Security.pdf

[31] Franz, Matthew, *Vulnerability Testing of Industrial Network Devices*, Critical Infrastructure Assurance Group, Cisco Systems, 2003, http://www.scadasec.net/oldio/papers/franz-isa-device-testing-oct03.pdf.

[32] Duggan, David, et al., *Penetration Testing of Industrial Control Systems*, Sandia National Laboratories, Report No SAND2005-2846P, 2005, http://www.sandia.gov/scada/documents/sand_2005_2846p.pdf.

[33] *21 Steps to Improve Cyber Security of SCADA Networks*, Office of Energy Assurance, U.S. Department of Energy, http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf.

[34] *TR99.00.01*: *Security Technologies for Manufacturing and Control Systems*, ISA, 2004.

Topic 4- ICS Security Program Development Section Post Quiz

Fill-in-the-Blank

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

2. A strong safety and _____is fundamental to a sustainable business model.

3. The importance of secure systems should be further emphasized as business reliance on _____ increases.

4. _____and malware (e.g., worms, viruses) have become all too common and have already impacted ICSs.

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

6. Cyber security programs with visible, top-level support from organization leaders are more likely to achieve_____, function more smoothly, and have earlier success than programs that do not have that support.

7. Whenever a new system is being designed and installed, it is imperative to take the time to address security throughout the lifecycle, from _____to installation to maintenance to decommissioning.

8. The cyber security team should identify the _____and computer systems within the ICS, as well as the networks within and interfacing to the ICS.

9. The _____will help identify any weaknesses that may be present in the systems that could allow the confidentiality, integrity, or availability of systems and data to be adversely affected, along with the related cyber security risks and mitigation approaches to reduce the risks.

10. A major concern is _____to devices and networks.

11. Vulnerability scanners often attempt to verify vulnerabilities by extensively probing and conducting a representative set of attacks against_____.

12. Identifying the vulnerabilities within an ICS requires a different approach than in a typical_____.

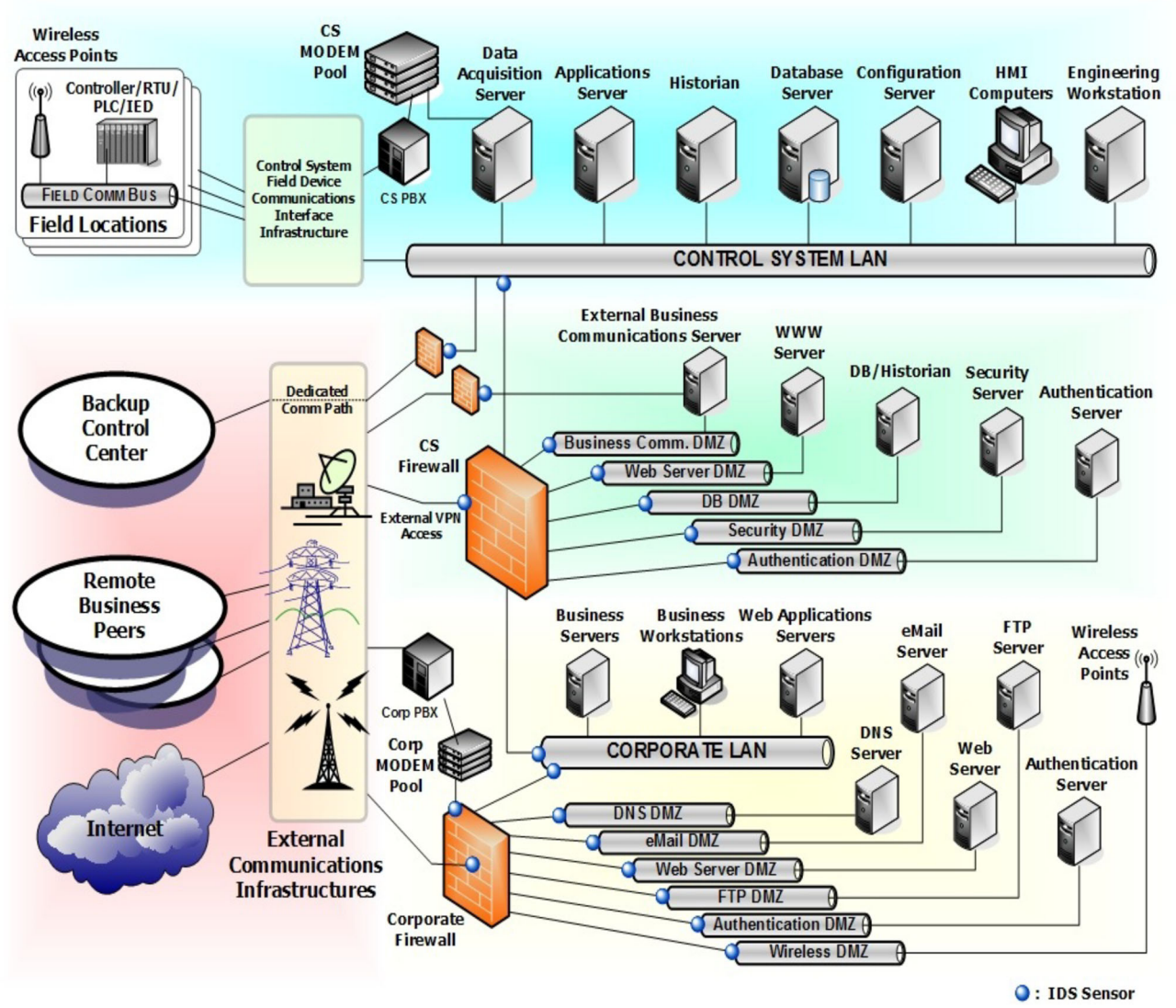
13. In most cases, devices on _____can be rebooted, restored, or replaced with little interruption of service to its customers.

14. An ICS controls a physical process and therefore has _____associated with its actions. Some actions are time-critical, while others have a more relaxed timeframe.

15. ICS systems have much greater _____than their IT counterparts have, so their hardware is often well behind the state-of-the-art and can be easily overtaxed..

Topic 5- Network Architecture Section

Topic 5 - Section Focus: You will learn the basics of the network design and security of the ICS program (Architecture). At the end of this section, you will be able to understand and describe the Network and Firewalls. There is a post quiz at the end of this section to review your comprehension and a final examination in the Assignment for your contact hours.
Topic 5 – Scope/Background: In an ICS environment, firewalls are most often deployed between the ICS network and the corporate network. Properly configured, they can greatly restrict undesired access to and from control system host computers and controllers, thereby improving security.



When designing a network architecture for an ICS deployment, it is usually recommended to separate the ICS network from the corporate network. The nature of network traffic on these two networks is different: Internet access, FTP, e-mail, and remote access will typically be permitted on the corporate network but should not be on the ICS network. Rigorous change control procedures for network equipment, configuration, and software changes may not be in place on the corporate network.

If ICS network traffic is carried on the corporate network, it could be intercepted or be subjected to a denial of service attack. By having separate networks, security and performance problems on the corporate network should not be able to affect the ICS network.

Practical considerations often mean that a connection is required between the ICS and corporate networks. This connection is a significant security risk and careful consideration should be given to the design.

If the networks must be connected, it is strongly recommended that only minimal (single if possible) connections be allowed and that the connection is through a firewall and a DMZ. A DMZ is a separate network segment that connects directly to the firewall. Servers containing the data from the ICS that needs to be accessed from the corporate network are put on this network segment.

Only these systems should be accessible from the corporate network. With any external connections, the minimum access should be permitted through the firewall, including opening only the ports required for specific communication. The following sections describe the access required for specific node types.

5.1 Firewalls

Network firewalls are devices or systems that control the flow of network traffic between networks employing differing security postures. In most modern applications, firewalls and firewall environments are discussed in the context of Internet connectivity and the TCP/IP protocol suite. However, firewalls have applicability in network environments that do not include or require Internet connectivity. For example, many corporate networks employ firewalls to restrict connectivity to and from internal networks servicing more sensitive functions, such as the accounting or personnel departments.

By employing firewalls to control connectivity to these areas, an organization can prevent unauthorized access to the respective systems and resources within the more sensitive areas.

There are three general classes of firewalls:

Packet Filtering Firewalls. The most basic type of firewall is called a packet filter. Packet filter firewalls are essentially routing devices that include access control functionality for system addresses and communication sessions. The access control is governed by a set of directives collectively referred to as a rule set. In their most basic form, packet filters operate at layer 3 (network) of the Open Systems Interconnection (OSI) model. This type of firewall checks basic information in each packet, such as IP addresses, against a set of criteria before forwarding the packet. Depending on the packet and the criteria, the firewall can drop the packet, forward it, or send a message to the originator. The advantages of packet filtering firewalls include low cost and low impact on network performance, usually because only one or a few header fields in the packet are examined.

Stateful Inspection Firewalls. Stateful inspection firewalls are packet filters that incorporate added awareness of the OSI model data at layer 4. Stateful inspection firewalls filter packets at the network layer, determine whether session packets are legitimate, and evaluate the contents of packets at the transport layer (e.g., TCP, UDP) as well. Stateful inspection keeps track of active sessions and uses that information to determine if packets should be forwarded or blocked. It offers a high level of security and good performance, but it may be more expensive and complex to administer. Additional rule sets for ICS applications may be required.

Application-Proxy Gateway Firewalls. This class of firewalls examines packets at the application layer and filters traffic based on specific application rules, such as specified applications (e.g., browsers) or protocols (e.g., FTP). It offers a high level of security, but could have overhead and delay impacts on network performance, which can be unacceptable in an ICS environment.

NIST SP 800-41, *Guidelines on Firewalls and Firewall Policy*, provides general guidance for the selection of firewalls and the firewall policies.

In an ICS environment, firewalls are most often deployed between the ICS network and the corporate network [34]. Properly configured, they can greatly restrict undesired access to and from control system host computers and controllers, thereby improving security. They can also potentially improve a control network's responsiveness by removing non-essential traffic from the network. When designed, configured, and maintained properly, dedicated hardware firewalls can contribute significantly to increasing the security of today's ICS environments.

Firewalls provide several tools to enforce a security policy that cannot be accomplished locally on the current set of process control devices available in the market, including the ability to:

- Block all communications with the exception of specifically enabled communications between devices on the unprotected LAN and protected ICS networks. Blocking is based on source and destination IP address pairs, services, and ports. Blocking can occur on both inbound and outbound packets, which is helpful in limiting high-risk communications such as e-mail.
- Enforce secure authentication of all users seeking to gain access to the ICS network. There is flexibility to employ varying protection levels of authentication methods including simple passwords, complex passwords, two-factor authentication technologies, tokens, biometrics and smart cards. Select the particular method based upon the vulnerability of the ICS network to be protected, rather than using the method that is available at the device level.
- Enforce destination authorization. Users can be restricted and allowed to reach only the nodes on the control network necessary for their job function. This reduces the potential of users intentionally or accidentally gaining access to and control of devices for which they are not authorized, but adds to the complexity for on-the-job-training or cross-training employees.
- Record information flow for traffic monitoring, analysis, and intrusion detection.
- Permit the ICS to implement operational policies appropriate to the ICS but that might not be appropriate in an IT network, such as prohibition of less secure communications like email, and permitted use of easy-to-remember usernames and group passwords.
- Be designed with documented and minimal (single if possible) connections that permit the ICS network to be severed from the corporate network, should that decision be made, in times of serious cyber incidents.

Other possible deployments include using either host-based firewalls or small standalone hardware firewalls in front of, or running on, individual control devices. Using firewalls on an individual device basis can create significant management overhead, especially in change management of firewall configurations.

There are several issues that must be addressed when deploying firewalls in ICS environments, particularly the following:

- The possible addition of delay to control system communications.
- The lack of experience in the design of rule sets suitable for industrial applications. Firewalls used to protect control systems should be configured so they do not permit either incoming or outgoing traffic by default. The default configuration should only be modified when it is necessary to permit connections to or from trusted systems.

Hardware firewalls do require ongoing support, maintenance, and backup. Rule sets need to be reviewed to make sure that they are providing adequate protection in light of ever-changing security threats.

System capabilities, such as available disk space, should be monitored to make sure that the firewall is performing its data collection tasks and can be depended upon in the event of a security violation. Real-time monitoring of firewalls and other security sensors is required to rapidly detect and initiate response to cyber incidents.

5.2 Logically Separated Control Network

The ICS network should, at a minimum, be logically separated from the corporate network on physically separate network devices. When enterprise connectivity is required:

- There should be documented and minimal (single if possible) access points between the ICS network and the corporate network. Redundant (i.e. backup) access points, if present, must be documented.
- A stateful firewall between the ICS network and corporate network should be configured to deny all traffic except that which is explicitly authorized.
- The firewall rules should at a minimum provide source and destination filtering (i.e. filter on media access control [MAC] address), in addition to TCP and User Datagram Protocol (UDP) port filtering and ICMP type and code filtering.

An acceptable approach to enabling communication between an ICS network and a corporate network is to implement an intermediate DMZ network. The DMZ should be connected to the firewall such that specific (restricted) communication may occur between only the corporate network and the DMZ, and the ICS network and the DMZ. The corporate network and the ICS network should not communicate directly with each other. This approach is described in Sections 5.3.4 and 5.3.5.

5.3 Network Segregation

ICS networks and corporate networks can be segregated to enhance cyber security using different architectures. This section describes several possible architectures and explains the advantages and disadvantages of each. Please note that intent of the diagrams in Section 5.3 is to show the placement of firewalls to segregate the network. Not all devices that would be typically found on the control network or corporate network are shown. Section 5.4 provides guidance on a recommend defense-in-depth architecture.

5.3.1 Dual-Homed Computer/Dual Network Interface Cards (NIC)

Dual-homed computers can pass network traffic from one network to another. A computer without proper security controls could pose additional threats. To prevent this, no systems other than firewalls should be configured as dual-homed to span both the control and corporate networks. All connections between the control network and the corporate network should be through a firewall.

5.3.2 Firewall between Corporate Network and Control Network

By introducing a simple two-port firewall between the corporate and control networks, as shown in Figure 5-1, a significant security improvement can be achieved. Firewalls usually offer stateful inspection for all TCP packets and application proxy services for common application layer protocols such as FTP, Hypertext Transfer Protocol (HTTP), and Simple Mail Transfer Protocol (SMTP). Properly configured, a firewall significantly reduces the chance of a successful external attack on the control network.

Unfortunately, two issues still remain with this design. First, if the data historian resides on the corporate network, the firewall must allow the data historian to communicate with the control devices on the control network. A packet originating from a malicious or incorrectly configured host on the corporate network (appearing to be the data historian) would be forwarded to individual PLCs/DCSs.

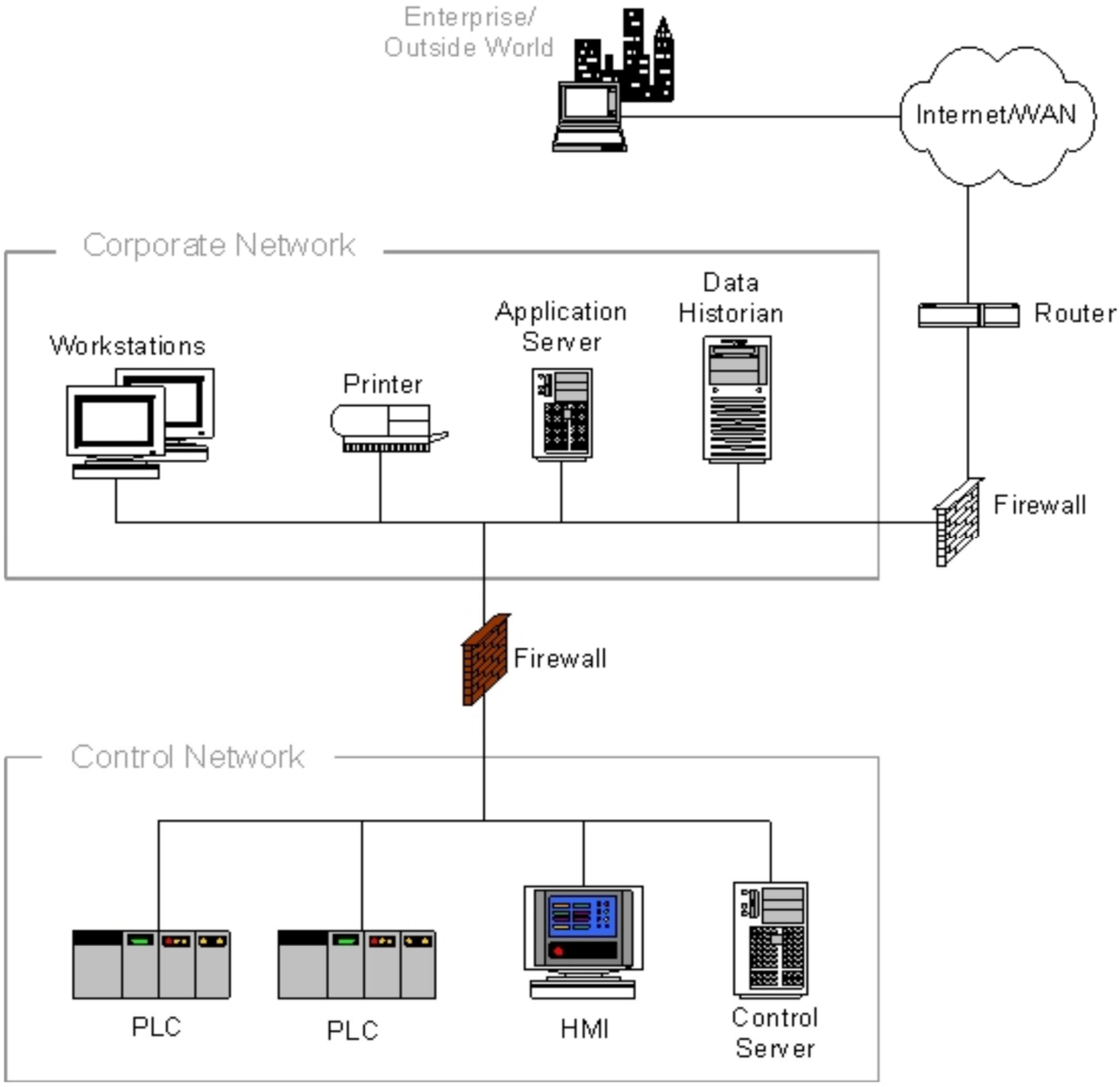


Figure 5-1. Firewall between Corporate Network and Control Network

If the data historian resides on the control network, a firewall rule must exist that allows all hosts from the enterprise to communicate with the historian. Typically, this communication occurs at the application layer as Structured Query Language (SQL) or HTTP requests. Flaws in the historian's application layer code could result in a compromised historian. Once the historian is compromised, the remaining nodes on the control network are vulnerable to a worm propagating or an interactive attack.

Another issue with having a simple firewall between the networks is that spoofed packets can be constructed that can affect the control network, potentially permitting covert data to be tunneled in allowed protocols.

For example, if HTTP packets are allowed through the firewall, then Trojan horse software accidentally introduced on an HMI or control network laptop could be controlled by a remote entity and send data (such as captured passwords) to that entity, disguised as legitimate traffic.

In summary, while this architecture is a significant improvement over a non-segregated network, it requires the use of firewall rules that allow direct communications between the corporate network and control network devices. This can result in possible security breaches if not very carefully designed and monitored [35].

5.3.3 Firewall and Router between Corporate Network and Control Network

A slightly more sophisticated design, shown in Figure 5-2, is the use of a router/firewall combination. The router sits in front of the firewall and offers basic packet filtering services, while the firewall handles the more complex issues using either stateful inspection or proxy techniques. This type of design is very popular in Internet-facing firewalls because it allows the faster router to handle the bulk of the incoming packets, especially in the case of DoS attacks, and reduces the load on the firewall. It also offers improved defense-in-depth since there are two different devices an adversary must bypass [35].

5.3.4 Firewall with DMZ between Corporate Network and Control Network

A significant improvement is the use of firewalls with the ability to establish a DMZ between the corporate and control networks. Each DMZ holds one or more critical components, such as the data historian, the wireless access point, or remote and third party access systems. In effect, the use of a DMZ-capable firewall allows the creation of an intermediate network.

Creating a DMZ requires that the firewall offer three or more interfaces, rather than the typical public and private interfaces. One of the interfaces is connected to the corporate network, the second to the control network, and the remaining interfaces to the shared or insecure devices such as the data historian server or wireless access points on the DMZ network. Figure 5-3 provides an example of this architecture.

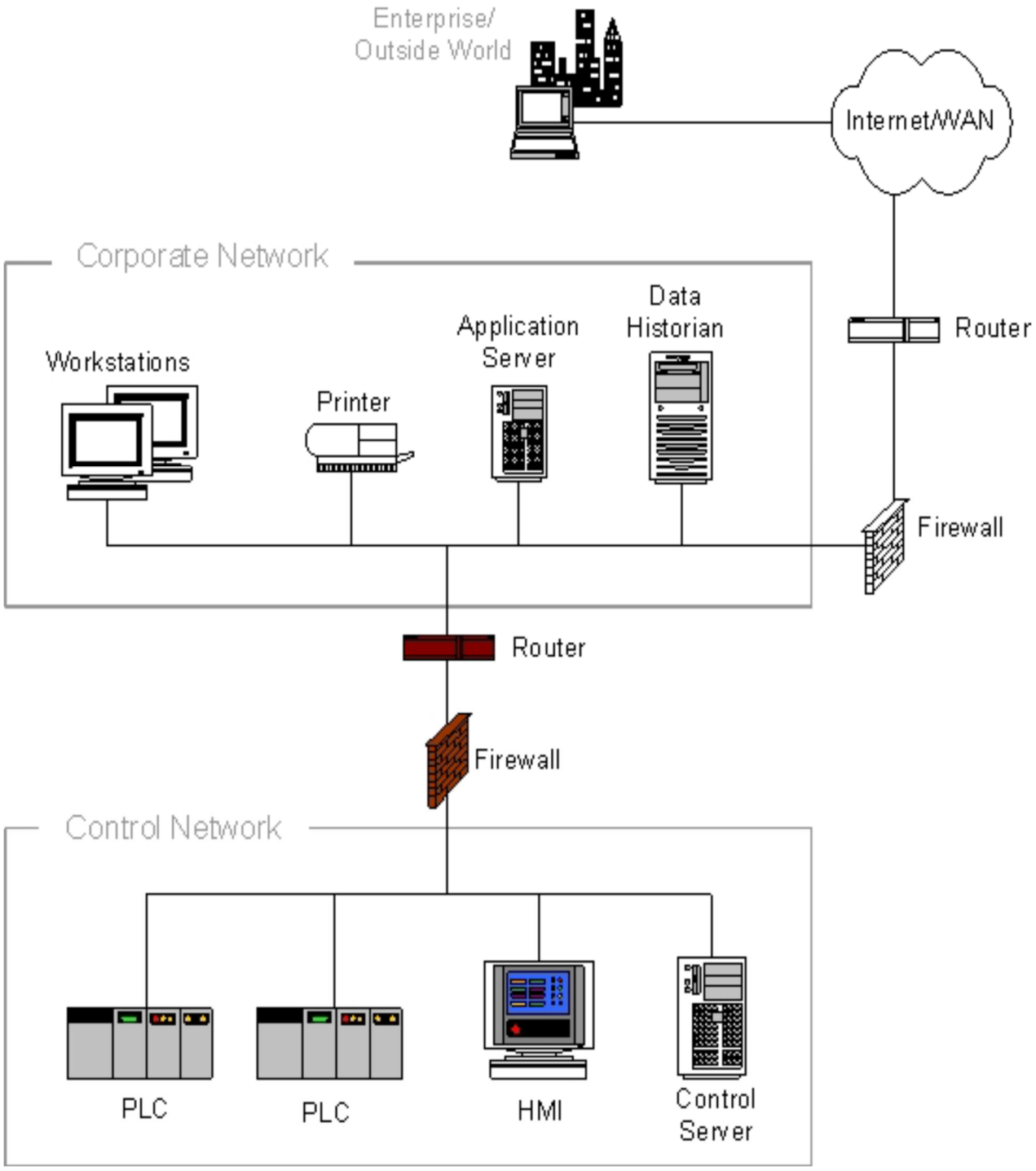


Figure 5-2. Firewall and Router between Corporate Network and Control Network

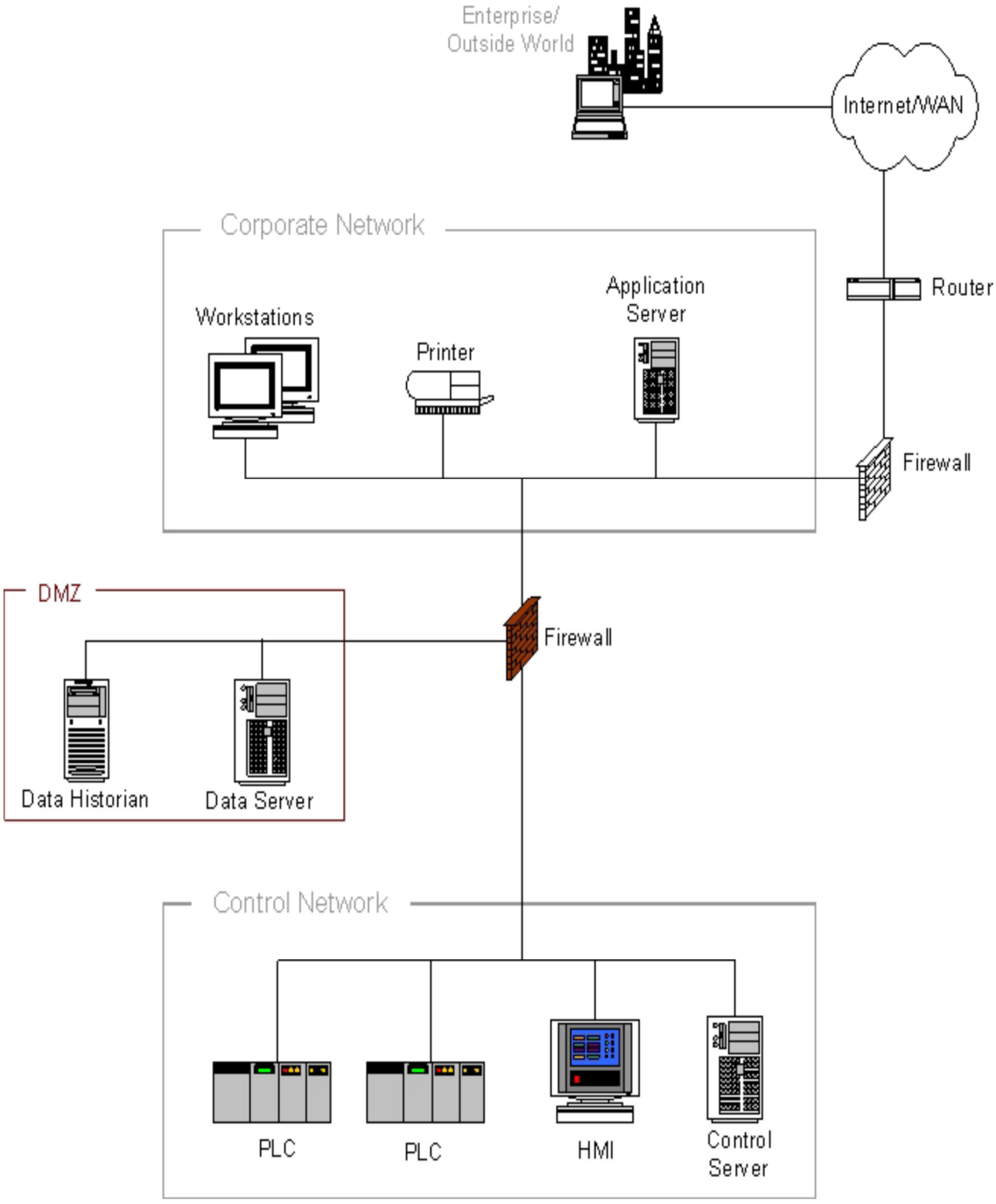


Figure 5-3. Firewall with DMZ between Corporate Network and Control Network

Patch Management Server

By placing corporate-accessible components in the DMZ, no direct communication paths are required from the corporate network to the control network; each path effectively ends in the DMZ. Most firewalls can allow for multiple DMZs, and can specify what type of traffic may be forwarded between zones.

As Figure 5-3 shows, the firewall can block arbitrary packets from the corporate network from entering the control network, and can also regulate traffic from the other network zones including the control network. With well-planned rule sets, a clear separation can be maintained between the control network and other networks, with little or no traffic passing directly between the corporate and control networks.

If a patch management server, an antivirus server, or other security server is to be used for the control network, it should be located directly on the DMZ. Both functions could reside on a single server.

Having patch management and antivirus management dedicated to the control network allows for controlled and secure updates that can be tailored for the unique needs of the ICS environment. It may also helpful if the antivirus product chosen for ICS protection is not the same as the antivirus product used for the corporate network.

For example, if a malware incident occurs and one antivirus product cannot detect or stop the malware, it is somewhat likely that another product may have that capability.

The primary security risk in this type of architecture is that if a computer in the DMZ is compromised, then it can be used to launch an attack against the control network via application traffic permitted from the DMZ to the control network. This risk can be greatly reduced if a concerted effort is made to harden and actively patch the servers in the DMZ and if the firewall rule set permits only connections between the control network and DMZ that are initiated by control network devices.

Other concerns with this architecture are the added complexity and the potential increased cost of firewalls with several ports. For more critical systems, however, the improved security should more than offset these disadvantages [35].

5.3.5 Paired Firewalls between Corporate Network and Control Network

A variation on the firewall with DMZ solution is to use a pair of firewalls positioned between the corporate and ICS networks, as shown in Figure 5-4. Common servers such as the data historian are situated between the firewalls in a DMZ-like network zone sometimes referred to as a Manufacturing Execution System (MES) layer.

As in the architectures described previously, the first firewall blocks arbitrary packets from proceeding to the control network or the shared historians. The second firewall can prevent unwanted traffic from a compromised server from entering the control network, and prevent control network traffic from impacting the shared servers.

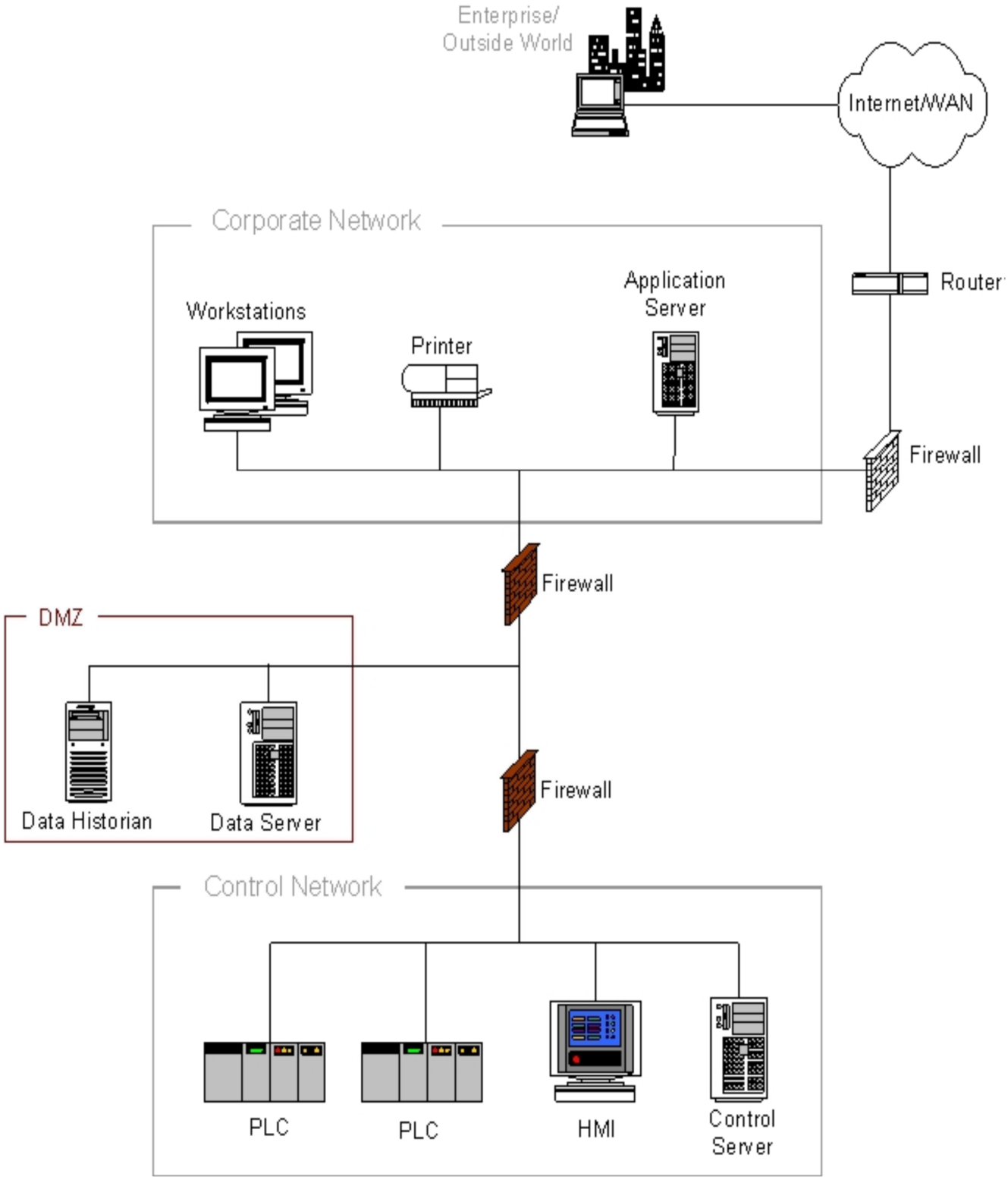


Figure 5-4. Paired Firewalls between Corporate Network and Control Network

If firewalls from two different manufacturers are used, then this solution may offer an advantage. It also allows the control group and the IT group to have clearly separated device responsibility since each can manage a firewall on its own, if the decision is made within the organization to do so. The primary disadvantage with two-firewall architectures is the increased cost and management complexity. For environments with stringent security requirements or the need for clear management separation, this architecture has some strong advantages.

5.3.6 Network Segregation Summary

In summary, non-firewall-based solutions will generally not provide suitable isolation between control networks and corporate networks. The two-zone solutions (no DMZ) are marginally acceptable but should be only be deployed with extreme care. The most secure, manageable, and scalable control network and corporate network segregation architectures are typically based on a system with at least three zones, incorporating a DMZ.

5.4 Recommended Defense-in-Depth Architecture

A single security product, technology or solution cannot adequately protect an ICS by itself. A multiple layer strategy involving two (or more) different overlapping security mechanisms, a technique also known as defense-in-depth, is desired so that the impact of a failure in any one mechanism is minimized.

A defense-in-depth architecture strategy includes the use of firewalls, the creation demilitarized zones, intrusion detection capabilities along with effective security policies, training programs and incident response mechanisms. In addition, an effective defense-in-depth strategy requires a thorough understanding of possible attack vectors on an ICS.

These include:

- Backdoors and holes in network perimeter
- Vulnerabilities in common protocols
- Attacks on Field Devices
- Database Attacks
- Communications hijacking and ‘Man-in-the-middle’ attacks

Figure 5-5 shows an ICS defense-in-depth architecture strategy that has been developed by the DHS Control Systems Security Program (CSSP) Recommended Practices committee17 as described in the *Control Systems Cyber Security: Defense in Depth Strategies* [36] document. Additional supporting documents that cover specific issues and associated mitigations are also included on the site. This site will continue to evolve and grow as new recommended practices and related information are added.

The *Control Systems Cyber Security: Defense in Depth Strategies* document provides guidance and direction for developing defense-in-depth architecture strategies for organizations that use control system networks while maintaining a multi-tier information architecture that requires:

- Maintenance of various field devices, telemetry collection, and/or industrial-level process systems
- Access to facilities via remote data link or modem
- Public facing services for customer or corporate operations

This strategy includes firewalls, the use of demilitarized zones and intrusion detection capabilities throughout the ICS architecture.

The use of several demilitarized zones in Figure 5-5 provides the added capability to separate functionalities and access privileges and has proved to be very effective in protecting large architectures comprised for networks with different operational mandates. Intrusion detection deployments apply different rule-sets and signatures unique to each domain being monitored.

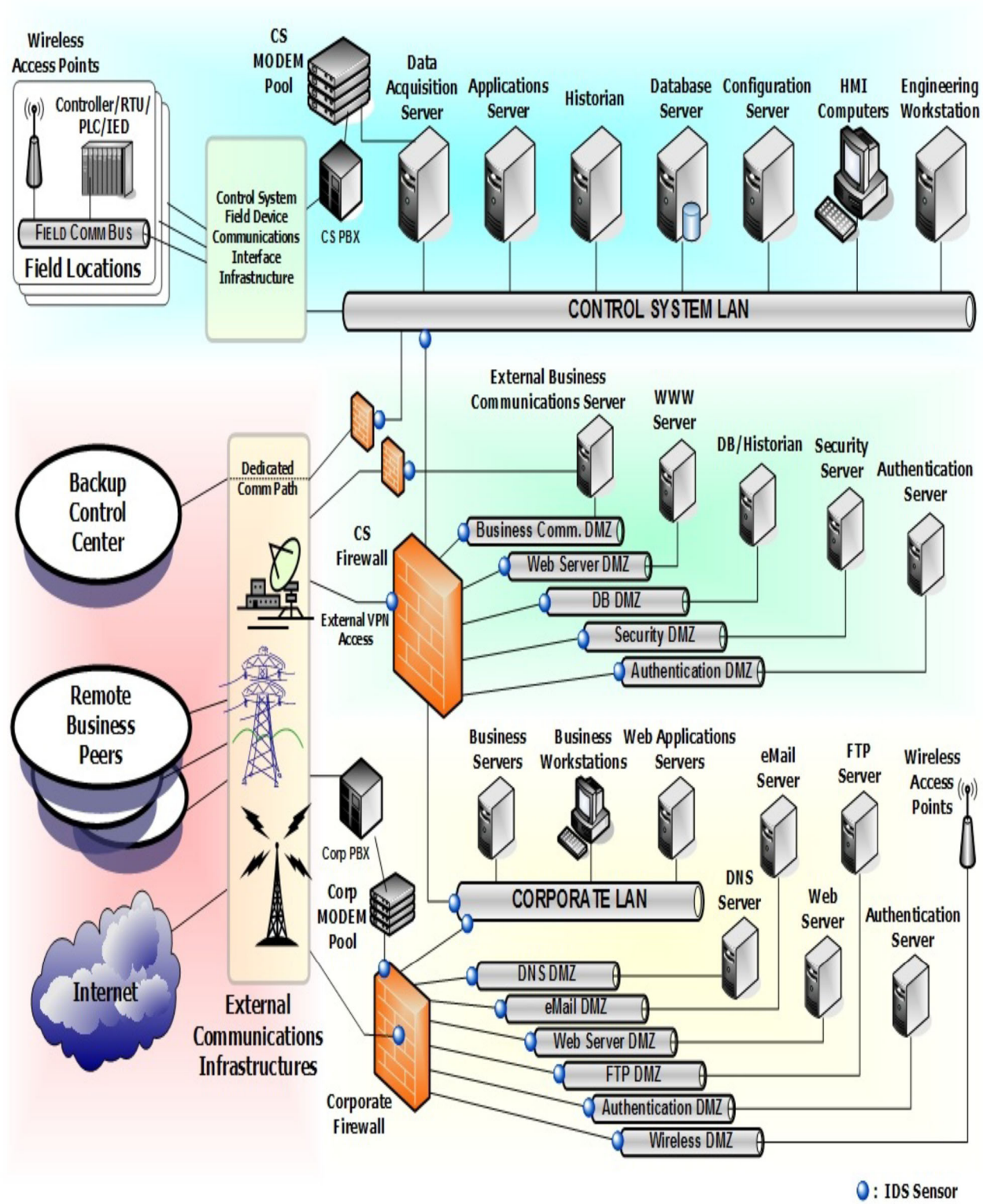


Figure 5-5. CSSP Recommended Defense-In-Depth Architecture

5.5 General Firewall Policies for ICS

Once the defense-in-depth architecture is in place, the work of determining exactly what traffic should be allowed through the firewalls begins. Configuring the firewalls to deny all except for the traffic absolutely required for business needs is every organization's basic premise, but the reality is much more difficult. Exactly what does "absolutely required for business" mean and what are the security impacts of allowing that traffic through? For example, many organizations considered allowing SQL traffic through the firewall as required for business for many data historian servers. Unfortunately, SQL was also the vector for the Slammer worm. Many important protocols used in the industrial world, such as HTTP, FTP, OPC/DCOM, EtherNet/IP, and MODBUS/TCP, have significant security vulnerabilities.

The remaining material in this section summarizes some of the key points from the *NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks* [35] document.

When installing a single two-port firewall without a DMZ for shared servers (i.e., the architecture described in Section 5.3.2), particular care needs to be taken with the rule design. At a minimum, all rules should be stateful rules that are both IP address and port (application) specific. The address portion of the rules should restrict incoming traffic to a very small set of shared devices (e.g., the data historian) on the control network from a controlled set of addresses on the corporate network. Allowing any IP addresses on the corporate network to access servers inside the control network is not recommended. In addition, the allowed ports should be carefully restricted to relatively secure protocols such as Hypertext Transfer Protocol Secure (HTTPS). Allowing HTTP, FTP, or any unencrypted SCADA protocol to cross the firewall is a security risk due to the potential for traffic sniffing and modification. Rules should be added to deny inbound communication with the control network. Rules should only allow devices internal to the control network the ability to establish connections outside the control network.

On the other hand, if the DMZ architecture is being used, then it is possible to configure the system so that no traffic will go directly between the corporate network and the control network. With a few special exceptions (noted below), all traffic from either side can terminate at the servers in the DMZ. This allows more flexibility in the protocols allowed through the firewall.

For example, MODBUS/TCP might be used to communicate from the PLCs to the data historian, while HTTP might be used for communication between the historian and enterprise clients. Both protocols are inherently insecure, yet in this case, they can be used safely because neither actually crosses between the two networks.

An extension to this concept is the idea of using "disjoint" protocols in all control network to corporate network communications. That is, if a protocol is allowed between the control network and DMZ, then it is explicitly **not** allowed between the DMZ and corporate network. This design greatly reduces the chance of a worm such as Slammer actually making its way into the control network, since the worm would have to use two different exploits over two different protocols.

One area of considerable variation in practice is the control of outbound traffic from the control network, which could represent a significant risk if unmanaged.

One example is Trojan horse software that uses HTTP tunneling to exploit poorly defined outbound rules.

Thus, it is important that outbound rules be as stringent as inbound rules. Appendix A of ISA's SP-99 Technical Report #2 [27] contains some example guidelines that help clarify this.

A summary of these follows:

- Inbound traffic to the control system should be blocked. Access to devices inside the control system should be through a DMZ.
- Outbound traffic through the control network firewall should be limited to essential communications only.
- All outbound traffic from the control network to the corporate network should be source and destination-restricted by service and port.

In addition to these rules, the firewall should be configured with outbound filtering to stop forged IP packets from leaving the control network or the DMZ. In practice this is achieved by checking the source IP addresses of outgoing packets against the firewall's respective network interface address. The intent is to prevent the control network from being the source of spoofed (i.e., forged) communications, which are often used in DoS attacks. Thus, the firewalls should be configured to forward IP packets only if those packets have a correct source IP address for the control network or DMZ networks. Finally, Internet access by devices on the control network should be strongly discouraged.

Summary

In summary, the following should be considered as recommended practice for general firewall rule sets:

- The base rule set should be deny all, permit none.
- Ports and services between the control network environment and the corporate network should be enabled and permissions granted on a specific case-by-case basis. There should be a documented business justification with risk analysis and a responsible person for each permitted incoming or outgoing data flow.
- All "permit" rules should be both IP address and TCP/UDP port specific, and stateful if appropriate.
- All rules should restrict traffic to a specific IP address or range of addresses.
- Traffic should be prevented from transiting directly from the control network to the corporate network. All traffic should terminate in the DMZ.
- Any protocol allowed between the control network and DMZ should explicitly NOT be allowed between the DMZ and corporate networks (and vice-versa).
- All outbound traffic from the control network to the corporate network should be source and destination-restricted by service and port.
- Outbound packets from the control network or DMZ should be allowed only if those packets have a correct source IP address that is assigned to the control network or DMZ devices.
- Control network devices should not be allowed to access the Internet.
- Control networks should not be directly connected to the Internet, even if protected via a firewall.
- All firewall management traffic should be carried on either a separate, secured management network (e.g., out of band) or over an encrypted network with two-factor authentication. Traffic should also be restricted by IP address to specific management stations.

These should only be considered as guidelines. A careful assessment of each control environment is required before implementing any firewall rule sets.

5.6 Recommended Firewall Rules for Specific Services

Beside the general rules described above, it is difficult to outline all-purpose rules for specific protocols. The needs and best practices vary significantly between industries for any given protocol and should be analyzed on an organization-by-organization basis. The Industrial Automation Open Networking Association (IAONA) offers a template for conducting such an analysis [37], assessing each of the protocols commonly found in industrial environments in terms of function, security risk, worst case impact, and suggested measures. Below are summarized some of the key points from the IAONA document, and suggested practices from the ISA TR2 Appendix A [27]. The reader is advised to consult these documents directly when developing rule sets.

5.6.1 Domain Name System (DNS)

Domain Name System (DNS) is primarily used to translate between domain names and IP addresses. For example, a DNS could map a domain name such as *control.com* to an IP address such as *192.168.1.1*. Most Internet services rely heavily on DNS, but its use on the plant floor is relatively rare at this time. In most cases, there is little reason to allow DNS requests out of the control network to the corporate network and no reason to allow DNS requests into the control network.

DNS requests from the control network to DMZ should be addressed on a case-by-case basis. Local DNS or the use of host files is recommended.

5.6.2 Hyper Text Transfer Protocol (HTTP)

HTTP is the protocol underlying Web browsing services on the Internet. Like DNS, it is critical to most Internet services. It is seeing increasing use on the plant floor as well as an all-purpose query tool. Unfortunately, it has little inherent security, and many HTTP applications have vulnerabilities that can be exploited. HTTP can be a transport mechanism for many manually performed attacks and automated worms.

In general, HTTP should not be allowed to cross from the corporate to the control network. If it is, then HTTP proxies should be configured on the firewall to block all inbound scripts and Java applications. Incoming HTTP connections should not be allowed into the control network, as they pose significant security risks. If HTTP services into the control network are absolutely required, it is recommended that the more secure HTTPS be used instead and only to specific devices.

5.6.3 FTP and Trivial File Transfer Protocol (TFTP)

FTP and Trivial File Transfer Protocol (TFTP) are used for transferring files between devices. They are implemented on almost every platform including many SCADA systems, DCSs, PLCs, and RTUs, since they are very well known and use minimum processing power. Unfortunately, neither protocol was created with security in mind; for FTP, the login password is not encrypted, and for TFTP, no login is required at all.

Furthermore, some FTP implementations have a history of buffer overflow vulnerabilities. As a result, all TFTP communications should be blocked, while FTP communications should be allowed for outbound sessions only or if secured with additional token-based two-factor authentication and an encrypted tunnel. More secure protocols, such as Secure Copy (SCP), should be employed whenever possible.

5.6.4 Telnet
The telnet protocol defines an interactive, text-based communications session between a client and a host. It is mainly used for remote login and simple control services to systems with limited resources or to systems with limited needs for security. It is a severe security risk because all telnet traffic, including passwords, is unencrypted, and it can allow a remote individual considerable control over a device.

Inbound telnet sessions from the corporate to the control network should be prohibited unless secured with token-based two-factor authentication and an encrypted tunnel. Outbound telnet sessions should be allowed only over encrypted tunnels to specific devices.

5.6.5 Simple Mail Transfer Protocol (SMTP)
SMTP is the primary e-mail transfer protocol on the Internet. E-mail messages often contain malware, so inbound e-mail should not be allowed to any control network device.

Outbound SMTP mail messages from the control network to the corporate network are acceptable to send alert messages.

5.6.6 Simple Network Management Protocol (SNMP)
SNMP is used to provide network management services between a central management console and network devices such as routers, printers, and PLCs. Although SNMP is an extremely useful service for maintaining a network, it is very weak in security.

Versions 1 and 2 of SNMP use unencrypted passwords to both read and configure devices (including devices such as PLCs), and in many cases the passwords are well known and cannot be changed. Version 3 is considerably more secure but is still limited in use. SNMP V1 & V2 commands both to and from the control network should be prohibited unless it is over a separate, secured management network whereas SNMP V3 commands may be able to be sent to the ICS using the security features inherent to V3.

5.6.7 Distributed Component Object Model (DCOM)
DCOM is the underlying protocol for both OLE for Process Control (OPC) and ProfiNet. It utilizes Microsoft's Remote Procedure Call (RPC) service, when not patched, has many vulnerabilities. These vulnerabilities were the basis for the Blaster worm exploits.

In addition, OPC, which utilizes DCOM, dynamically opens a wide range of ports (1024 to 65535) that can be extremely difficult to filter at the firewall. This protocol should only be allowed between control network and DMZ networks and explicitly blocked between the DMZ and corporate network. In addition, users are advised to restrict the port ranges used by making registry modifications on devices using DCOM.

5.6.8 SCADA and Industrial Protocols
SCADA and industrial protocols, such as MODBUS/TCP, EtherNet/IP, and DNP3, are critical for communications to most control devices. Unfortunately, these protocols were designed without security in mind and do not typically require any authentication to remotely execute commands on a control device. These protocols should only be allowed within the control network and not allowed to cross into the corporate network.

5.7 Network Address Translation (NAT)

Network address translation (NAT) is a service where IP addresses used on one side of a network device can be mapped to a different set on the other side on an as-needed basis. It was originally designed for IP address reduction purposes so that an organization with a large number of devices that occasionally needed Internet access could get by with a smaller set of assigned Internet addresses.

To do this, NAT relies on the premise that not every internal device is actively communicating with external hosts at a given moment. The firewall is configured to have a limited number of outwardly visible IP addresses.

When an internal host seeks to communicate to an external host, the firewall remaps the internal IP address and port to one of the currently unused, more limited, public IP addresses, effectively concentrating outgoing traffic into fewer IP addresses.

The firewall must track the state of each connection and how each private internal IP address and source port was remapped onto an outwardly visible IP address/port pair. When returning traffic reaches the firewall, the mapping is reversed and the packets forwarded to the proper internal host.

For example, a control network device may need to establish a connection with an external, non-control network host (for instance, to send a critical alert e-mail). NAT allows the internal IP address of the initiating control network host to be replaced by the firewall; subsequent return traffic packets are remapped back to the internal IP address and sent to the appropriate control network device.

More specifically, if the control network is assigned the private subnet 192.168.1.xxx and the Internet network expects the device to use the corporate assigned addresses in the range 192.6.yyy.zzz, then a NAT generated by a control network device.

Producer-consumer protocols, such as EtherNet/IP and Foundation Fieldbus, are particularly troublesome because NAT does not support the multicast-based traffic that these protocols need to offer their full services.

In general, while NAT offers some distinct advantages, its impact on the actual industrial protocols and configuration should be assessed carefully before it is deployed. Furthermore, certain protocols are specifically broken by NAT because of the lack of direct addressing. For example, OPC requires special third-party tunneling software to work with NAT.

5.8 Specific ICS Firewall Issues

In addition to the issues with firewalls and ICSs already discussed in this section, there are some additional problems that need to be examined in more detail. The rest of this section discusses three specific areas of concern: the placement of data historians, remote access for ICS support, and multicast traffic.

5.8.1 Data Historians

The existence of shared control network/corporate network servers such as data historians and asset management servers can have a significant impact on firewall design and configuration. In three-zone systems, the placement of these servers in a DMZ is relatively straightforward, but in two-zone designs the issues become complex.

Placing the historian on the corporate side of the firewall means that a number of insecure protocols, such as MODBUS/TCP or DCOM, must be allowed through the firewall and that every control device reporting to the historian is exposed to the corporate side of the network. On the other hand, putting the historian on the control network side means other equally questionable protocols, such as HTTP or SQL, must be allowed through the firewall, and there is now a server accessible to nearly everyone in the organization sitting on the control network.

In general, the best solution is to avoid two-zone systems (no DMZ) and use a three-zone design, placing the data collector in the control network and the historian component in the DMZ; however, even this can prove problematic in some situations. Heavy access from the large numbers of users on the corporate network to a historian in the DMZ may tax the firewall's throughput capabilities.

One potential solution is to install two servers: one on the control network to collect data from the control devices, and a second on the corporate network mirroring the first server and supporting client queries. The issue of how to time synchronize both historians will have to be addressed. This also requires a special hole to be put through the firewall to allow direct server-to-server communications, but if done correctly, this poses only minor risk.

5.8.2 Remote Support Access

Another issue for ICS firewall design is user and/or vendor remote access into the control network. Any users accessing the control network from remote networks should be required to authenticate using an appropriately strong mechanism such as token-based authentication. While it is possible for the controls group to set up their own remote access system with two-factor authentication on the DMZ, in most organizations it is typically more efficient to use existing systems set up by the IT department. In this case, a connection through the firewall from the IT remote access server is needed.

Remote support personnel connecting over the Internet or via dialup modems should use an encrypted protocol, such as running a corporate VPN connection client, Citrix, or secure HTTP access, and authenticate using a strong mechanism, such as a token based two-factor authentication scheme, in order to connect to the general corporate network. Once connected, they should be required to authenticate a second time at the control network firewall using a strong mechanism, such as a token based two-factor authentication scheme, to gain access to the control network.

For organizations that do not allow any control traffic to traverse the corporate network in the clear, this could require a cascading, or secondary tunneling solutions, to gain access to the control network, such as an SSL VPN inside an IPsec VPN.

5.8.3 Multicast Traffic

Most industrial producer-consumer (or publisher-subscriber) protocols operating over Ethernet, such as EtherNet/IP and Foundation Fieldbus HSE, are IP multicast-based. The first advantage of IP multicasting is network efficiency; by not repeating the data transmission to the multiple destinations, a significant reduction in network load can occur.

The second advantage is that the sending host need not be concerned with knowing every IP address of every destination host listening for the broadcast information. The third, and perhaps most important for industrial control purposes, is that a single multicast message offers far better capabilities for time synchronization between multiple control devices than multiple unicast messages.

If the source and destinations of a multicast packet are connected with no intervening routers or firewalls between them, the multicast transmission is relatively seamless. However, if the source and destinations are not on the same LAN, forwarding the multicast messages to a destination becomes more complicated.

To solve the problem of multicast message routing, hosts need to join (or leave) a group by informing the multicast router on their network of the relevant group ID through the use of the Internet Group Management Protocol (IGMP).

Multicast routers subsequently know of the members of multicast groups on their network and can decide whether or not to forward a received multicast message onto their network. A multicast routing protocol is also required. From a firewall administration perspective, monitoring and filtering IGMP traffic becomes another series of rule sets to manage, adding to the complexity of the firewall.

Another firewall issue related to multicasting is the use of NAT. A firewall performing NAT that receives a multicast packet from an external host has no reverse mapping for which internal group ID should receive the data. If IGMP-aware, it could broadcast it to every group ID it knows about, since one of them will be correct, but this could cause serious issues if an unintended control packet were broadcast to a critical node.

The safest action for the firewall to take is to drop the packet. Thus, multicasting is generally considered NAT-unfriendly.

Encryption

As a longer-term solution, systems should be designed to include encryption between devices in order to make it very difficult to reverse engineer protocols and forge packets on control system networks. Encrypting the communications between devices would make it nearly impossible to perform this attack.

Monitoring

Monitoring for ARP poisoning provides an added layer of defense. There are several programs available (e.g., ARPwatch) that can monitor for changing MAC addresses through the ARP packets.

5.9 Single Points of Failure

Single points of failure can exist at any level of the ANSI/ISO stack. An example is PLC control of safety interlocks. Since security is usually being added to the ICS environment, an evaluation should be done to identity potential failure points and a risk assessment done to evaluate each point's exposure. Remediation methods can then be postulated and evaluated and a "risk versus reward" determination made and design and implementation done.

5.10 Redundancy and Fault Tolerance

ICS components or networks that are classified as critical to the organization have high availability requirements. One method of achieving high availability is through the use of redundancy. Additionally, if a component fails, it should fail in a manner that does not generate unnecessary traffic on the ICS, or does not cause another problem elsewhere, such as a cascading event.

The control system should have the ability to execute an appropriate fail-safe process upon the loss of communications with the ICS or the loss of the ICS itself. The organization should define what "loss of communications" means (e.g., 5 seconds, 5 minutes, etc. without communications). The organization should then define the appropriate fail-safe process for their industry.

Backups should be performed using the "backup-in-depth" approach, with layers of backups (e.g., local, facility, disaster, etc.) that are time-sequenced such that rapid recent local backups are available for immediate use and secure backups are available to recover from a massive security incident. A mixture of backup/restore approaches and storage methods should be used to ensure that backups are rigorously produced, securely stored, and appropriately accessible for restoration.

5.11 Preventing Man-in-the-Middle Attacks

A Man-in-the-Middle attack requires the use the Address Resolution Protocol (ARP) and knowledge of the protocol being manipulated. The ARP Man-in-the-Middle attack is a popular method for an adversary to gain access to the network flow of information on a target system. This is performed by attacking the network ARP cache tables of the controller and the workstation machines.

Using the compromised computer on the control network, the adversary poisons the ARP tables on each host and informs them that they must route all their traffic through a specific IP and hardware address (i.e., the adversary's machine). By manipulating the ARP tables, the adversary can insert his machine between the two target machines and/or devices.

The Man-in-the-Middle attack works by initiating gratuitous ARP commands to confuse each host (i.e., ARP poisoning). These ARP commands cause each of the two target hosts to use the MAC address of the adversary as the address for the other target host. When a successful Man-in-the-Middle attack is performed, the hosts on each side of the attack are unaware that their network data is taking a different route through the adversary's computer.

Once an adversary has successfully inserted their machine into the information stream, they now have full control over the data communications and could carry out several types of attacks. One possible attack method is the replay attack. In its simplest form, captured data from the control/HMI is modified to instantiate activity when received by the device controller.

Captured data reflecting normal operations in the ICS could be played back to the operator as required. This would cause the operator's HMI to appear to be normal and the attack will go unobserved. During this replay attack the adversary could continue to send commands to the controller and/or field devices to cause an undesirable event while the operator is unaware of the true state of the system.

Another attack that could be carried out with the Man-in-the-Middle attack is sending false messages to the operator, and could take the form of a false negative or a false positive. This may cause the operator to take an action, such as flipping a breaker, when it is not required, or it may cause the operator to think everything is fine and not take an action when an action is required. The adversary could send commands to the operator's console indicating a system change, and when the operator follows normal procedures and attempts to correct the problem, the operator's action could cause an undesirable event. There are numerable variations of the modification and replay of control data could impact the operations of the system.

Protocol manipulation and the Man-in-the-Middle attack tare among the most popular ways to manipulate insecure protocols, such as those found in control systems. However, there are mitigation techniques [38] that can be applied to secure the systems through MAC address locking, static tables, encryption, and monitoring.

Mac Locking

The ARP Man-in-the-Middle attack requires the adversary to be connected to the local network or have control of a local computer on the network. Port security, also called MAC address locking, is one method to secure the physical connection at the end of each port on a network switch. The high-end corporate class network switches usually have some kind of option for MAC address locking. MAC address locking is very effective against a rogue individual looking to physically plug into the internal network.

Without port security, any open network jack on the wall could be used as an avenue onto the corporate network. Port security locks a specific MAC address to a specific port on a managed switch. If the MAC address does not match, the communication link is disabled and the intruder will not be able to achieve his goal. Some of the more advanced switches have an auto resetting option, which will reset the security measure if the original MAC is returned to the port.

Although port security is not attacker proof, it does add a layer of added security to the physical network. It also protects the local network from employees plugging un-patched and out-of-date systems onto the protected network. This reduces the number of target computers a remote adversary can access. These security measures not only protect against attacks from external networks but provide added physical protection as well.

Static Tables

An ICS network that stays relatively static could attempt to implement statically coded ARP tables. Most operating systems have the capability to statically code all of the MAC addresses into the ARP table on each computer. Statically coding the ARP tables on each computer prevents the adversary from changing them by sending ARP reply packets to the victim computer. While this technique is not feasible on a large and/or dynamic corporate network, the limited number of hosts on an ICS network could be effectively protected this way.

Topic 5- Network Architecture Section References

GUIDE TO SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) AND INDUSTRIAL CONTROL SYSTEMS SECURITY

[32] Duggan, David, et al., *Penetration Testing of Industrial Control Systems*, Sandia National Laboratories, Report No SAND2005-2846P, 2005, http://www.sandia.gov/scada/documents/sand_2005_2846p.pdf.

[33] *21 Steps to Improve Cyber Security of SCADA Networks*, Office of Energy Assurance, U.S. Department of Energy, http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf.

[34] *TR99.00.01*: *Security Technologies for Manufacturing and Control Systems*, ISA, 2004.

[35] *NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks*, National Infrastructure Security Coordination Centre, London, 2005, http://www.niscc.gov.uk/niscc/docs/re-20050223-00157.pdf.

[36] Idaho National Laboratory, *Control Systems Cyber Security: Defense in Depth Strategies*, Homeland Security External Report # INL/EXT-06-11478, May 2006, http://csrp.inl.gov/Documents/Defense%20in%20Depth%20Strategies.pdf

[37] *The IAONA Handbook for Network Security – Draft/RFC v0.4*, Industrial Automation Open Networking Association (IAONA), Magdeburg, Germany, 2003.

[38] Idaho National Laboratory, *Common Control System Vulnerability*, Homeland Security External Report # INL/EXT-05-00993, November 2005, www.us-cert.gov/control_systems/pdf/csvul1105.pdf

[39] NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, 1995, http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf.

[40] Mell, Peter, et al., NIST SP 800-40 Version 2, *Creating a Patch and Vulnerability Management Program,* 2005, http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf.

[41] Wack, John, et al., NIST SP 800-42, *Guideline on Network Security Testing*, 2003, http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf.

[42] Roback, Edward, NIST SP 800-23, *Guidelines to Federal Organizations on Security Assurance and Acquisition/ Use of Tested/Evaluated Products*, 2000, http://csrc.nist.gov/publications/nistpubs/800-23/sp800-23.pdf.

[43] Stoneburner, Gary, et al., NIST SP 800-27, *Engineering Principles for Information Security (A Baseline for Achieving Security), Revision A*, 2004, http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.

[44] Grance, Tim, et al., NIST SP 800-35, *Guide to Information Technology Security Services*, 2003, http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf.

Topic 5- Network Architecture Section Post Quiz

Fill-in-the Blank

1. If ICS network traffic is carried on the_____, it could be intercepted or be subjected to a denial of service attack.

2. By having separate networks, _____problems on the corporate network should not be able to affect the ICS network.

3. If the networks must be connected, it is strongly recommended that only minimal (single if possible) connections be allowed and that the connection is through a firewall and a_____.

4. A DMZ is a _____that connects directly to the firewall.

5. Servers containing the data from the _____that needs to be accessed from the corporate network are put on this network segment.

6. With any external connections, the minimum access should be permitted through the firewall, including opening only the _____required for specific communication.

7. _____ are devices or systems that control the flow of network traffic between networks employing differing security postures.

8. In most modern applications, firewalls and firewall environments are discussed in the context of Internet connectivity and the_____.

9. By employing firewalls to control connectivity to these areas, an organization can prevent _____to the respective systems and resources within the more sensitive areas.

10. In an ICS environment, firewalls are most often deployed between the ICS network and the _____ network.

11. Properly configured, they can greatly restrict undesired access to and from control system host computers and controllers, thereby improving_____.

12. The _____network should, at a minimum, be logically separated from the corporate network on physically separate network devices.

13. An acceptable approach to enabling communication between an ICS network and a corporate network is to implement _____ network.

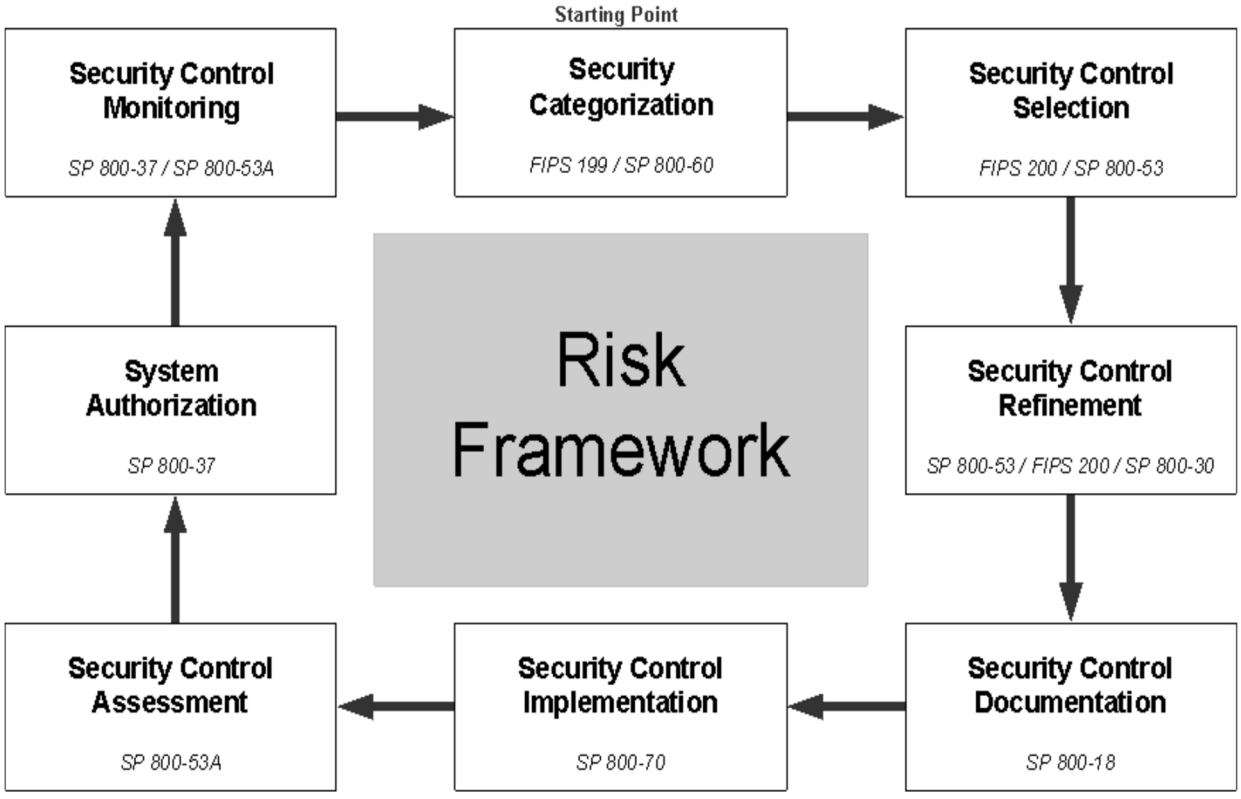
14. ICS networks and corporate networks can be segregated to enhance cyber security using different_____ .

15. If the _____resides on the control network, a firewall rule must exist that allows all hosts from the enterprise to communicate with the historian.

Topic 6 – ICS Security Controls Section

Topic 6 - Section Focus: You will learn the basics of the ICS security control. At the end of this section, you will be able to understand and describe security controls are the management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an informational system to protect the confidentiality, integrity, and availability of the system and its information.

Topic 6 – Scope/Background: An effective cyber security strategy for an ICS should apply defense-in-depth, a technique of layering security mechanisms so that the impact of a failure in any one mechanism is minimized. Use of such a strategy is explored within the security control discussions and their applications to ICS that follow.



Risk Framework Diagram

Security controls are the management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an informational system to protect the confidentiality, integrity, and availability of the system and its information.

This section discusses the security controls specified in NIST SP 800-53, which was developed as part of the FISMA implementation project. See Appendix E for additional information regarding FISMA and the NIST-led implementation project.

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

NIST has initiated a high-priority project18 in cooperation with the public and private sector ICS community to develop specific guidance on the application of the security controls in NIST SP 800-53 to ICSs. Since the project is still ongoing, the resulting guidance could not be included in the current release of this document or NIST SP 800-53, but will appear in future releases. Initial ICS specific recommendations and guidance, if available, will be provided in an outlined box for each section.

A single security product or technology cannot adequately protect an ICS. Securing an ICS is based on a combination of effective security policies and a properly configured set of security controls.

An effective cyber security strategy for an ICS should apply defense-in-depth, a technique of layering security mechanisms so that the impact of a failure in any one mechanism is minimized. Use of such a strategy is explored within the security control discussions and their applications to ICS that follow.

6.1 Management Controls

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

Risk Assessment (RA): the process of identifying risks to operations, assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact

Planning (PL): development and maintenance of a plan to address information system security by performing assessments, specifying and implementing security controls, assigning security levels, and responding to incidents

System and Services Acquisition (SA): allocation of resources for information system security to be maintained throughout the systems life cycle and the development of acquisition policies based on risk assessment results including requirements, design criteria, test procedures, and associated documentation

Certification, Accreditation, and Security Assessments (CA): assurance that the specified controls are implemented correctly, operating as intended, and producing the desired outcome.

These management controls are discussed in more detail in the sections to follow. Initial ICS specific recommendations and guidance, if available, will be provided in an outlined box for each section.

6.1.1 Risk Assessment

Risk is a function of the likelihood of a given threat source exploiting a potential vulnerability and the resulting impact of exploiting this vulnerability. Risk assessment is the process of identifying risks to an organization's operations, assets, and individuals by determining the probability of occurrence that an identified threat will exploit an identified vulnerability and the resulting impact. An assessment includes an evaluation of security controls that can mitigate each threat and the costs associated with implementing them. A risk assessment must also compare the cost of security with the costs associated with an incident.

Achieving an acceptable level of risk is a process of reducing the probability of an incident that is accomplished by mitigating or eliminating vulnerabilities that can be exploited as well as consequences resulting from an incident. Prioritization of vulnerabilities must be based on cost and benefit with an objective to provide a business case for implementing at least a minimum set of control system security requirements to reduce risk to an acceptable level. A mistake often made during a risk assessment is to select technically interesting vulnerabilities without taking into account the level of risk associated with them. Vulnerabilities should be assessed and rated for risk before trying to select and implement security controls on them.

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

In the FISMA Risk Framework shown in Figure E-1 in Appendix E, the risk assessment process is applied after the Security Categorization activity and baseline Security Control Selection activity. Risk assessment is performed in the Security Control Refinement activity to determine if the selected security controls need to be enhanced or expanded beyond the baseline security controls. NIST SP 800-30, *Risk Management Guide for Information Technology Systems* (currently under revision) provides a risk assessment methodology, which includes the following steps:

1. System characterization – produces a picture of the information system environment, and delineation of system boundaries
2. Threat identification – produces a threat statement containing a list of threat-sources that could exploit system vulnerabilities
3. Vulnerability identification – produces a list of the system vulnerabilities that could be exercised by the potential threat sources
4. Control analysis – produces a list of the planned controls used for the information system to mitigate the likelihood of a vulnerability being exercised and reduce the impact of such an adverse event.
5. Likelihood determination – produces a likelihood rating (High, Medium, or Low) that indicates the probability that a potential vulnerability may be exercised
6. Impact analysis – produces a magnitude of impact (High, Medium, or Low) resulting from the exploitation of a vulnerability.

7. Risk determination – produces measurement for risk based on a scale of high, medium, or low
8. Control recommendations – produces recommendations of security controls and alternative solutions to mitigate risk
9. Results documentation – produces a risk assessment report that describes the threats and vulnerabilities, measures the risk, and provides recommendations for control implementation.

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

- NIST SP 800-12 provides guidance on security policies and procedures [39].
- NIST SP 800-30 provides guidance on conducting risk assessments and updates [19].
- NIST SP 800-40 provides guidance on handling security patches [40].
- NIST SP 800-42 provides guidance on network security testing [41].
- NIST SP 800-60 provides guidance on determining security categories for information types [24].

ICS Specific Recommendations and Guidance

Organizations must consider the potential consequences resulting from an incident on an ICS. Well-defined policy and procedures lead to mitigation techniques designed to thwart incidents and manage the risk to eliminate or minimize the consequences. The degradation of the physical plant, economic status, or national confidence could justify mitigation. For an ICS, a very important aspect of the risk assessment is to determine the value of the data that is flowing from the control network to the corporate network. In instances where pricing decisions are determined from this data, the data could have a very high value.

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

6.1.2 Planning

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

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

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

- NIST SP 800-12 provides guidance on security policies and procedures [39].
- NIST SP 800-18 provides guidance on preparing rules of behavior [17].

ICS Specific Recommendations and Guidance
A security plan for an ICS should build on appropriate existing IT security experience, programs, and practices. However, the critical differences between IT and ICS addressed in Section 3.1 will influence how security will be applied to the ICS. A forward-looking plan is needed to provide a method for continuous security improvements. ICS security is a rapidly evolving field requiring the security planning process to constantly explore emerging ICS security capabilities as well as new threats that identified by organizations such as the US-CERT Control Systems Security Center (CSSC).

In support of the acquisition of secured ICS, the Process Control Security Requirements Forum (PCSRF), an industry-based effort being lead by NIST, has documented a cohesive, cross-industry set of requirements for new ICS [48] with follow-up work addressing SCADA and subcomponent-level requirements.

The SCADA and Control System Procurement Project [49] is also developing a procurement language for specifying security requirements when procuring new systems or maintaining existing systems.

The security requirements of an organization outsourcing the management and control of all or some of its information systems, networks, and desktop environments should be addressed in a contract agreed between the parties. External suppliers that have an impact on the security of the organization must be held to the same security policies and procedures to maintain the overall level of ICS security. Security policies and procedures of second and third-tier suppliers should also be in compliance with corporate cyber security policies and procedures in the case that they impact ICS security.

6.1.4 Certification, Accreditation, and Security Assessments
The security controls that fall within the NIST SP 800-53 Certification, Accreditation, and Security Assessments (CA) family provide the basis for performing periodic assessments and providing certification of the security controls implemented in the information system to determine if the controls are implemented correctly, operating as intended, and producing the desired outcome to meet the system security requirements. This assessment should also include all connections from the information system under consideration to other information systems that are inside the boundary of the information system under consideration.

A senior organizational official is responsible for accepting residual risk and authorizing system operation. These steps constitute accreditation. In addition, all security controls should be monitored on an ongoing basis. Monitoring activities include configuration management and control of information system components, security impact analysis of changes to the system, ongoing assessment of security controls, and status reporting.

Supplemental guidance for the CA controls can be found in the following documents:
- NIST SP 800-12 provides guidance on security policies and procedures [39].
- NIST SP 800-26 and 800-53A provide guidance on security control assessments [18][22].
- NIST SP 800-37 provides guidance defining the information system boundary and security certification and accreditation of the information system [20].

6.2 Operational Controls

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

Personnel Security (PS): policy and procedures for personnel position categorization, screening, transfer, penalty, and termination; also addresses third-party personnel security.

Physical and Environmental Protection (PE): policy addressing physical, transmission, and display access control as well as environmental controls for conditioning (e.g., temperature, humidity) and emergency provisions (e.g., shutdown, power, lighting, fire protection).

Contingency Planning (CP): policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.

Configuration Management (CM): policy and procedures for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation.

Maintenance (MA): policies and procedures to manage all maintenance aspects of an information system.

System and Information Integrity (SI): policy and procedures to protect information systems and their data from design flaws and data modification using functionality verification, data integrity checking, intrusion detection, malicious code detection, and security alert and advisory controls.

Media Protection (MP): policy and procedures to ensure secure handling of media. Controls cover access, labeling, storage, transport, sanitization, destruction, and disposal.

Incident Response (IR): policy and procedures pertaining to incident response training, testing, handling, monitoring, reporting, and support services.

Awareness and Training (AT): policies and procedures to ensure that all information system users are given appropriate security training relative to their usage of the system and that accurate training records are maintained.

These operational controls are discussed in more detail in the sections to follow. Initial ICS specific recommendations and guidance, if available, will be provided in an outlined box for each section.

6.2.1 Personnel Security

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

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

- NIST SP 800-12 provides guidance on security policies and procedures [39].
- NIST SP 800-35 provides guidance on information technology security services [44].
- NIST SP 800-73 provides guidance on interfaces for personal identity verification [50].
- NIST SP 800-76 provides guidance on biometrics for personal identity verification [51].

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

Hiring Policies

This includes pre-employment screening such as background checks, the interview process, hiring policies, complete job descriptions and detailing of duties, terms and condition of employment, and legal rights and responsibilities of employees or contractors.

Organization Policies and Practices

These include security policies, information classification, document and media maintenance and handling policies, user training, acceptable usage policies for organization assets, periodic employee performance reviews, appropriate background checks, and any other policies and actions that detail expected and required behavior of organization employees, contractors, and visitors. Organization policies to be enforced should be written down and readily available to all workers through an employee handbook, distributed as e-mail notices, located in a centralized resource area, or posted directly at a worker's area of responsibility.

Terms and Conditions of Employment

This category includes job and position responsibilities, notification to employees of terminable offenses, disciplinary actions and punishments, and periodic employee performance reviews.

ICS Specific Recommendations and Guidance

Positions should be categorized with a risk designation and screening criteria, and individuals filling a position should be screened against this criteria as well as complete an access agreement before being granted access to an information system. Personnel should be screened for the critical positions controlling and maintaining the ICS.

6.2.2 Physical and Environmental Protection

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

This family also includes controls for the deployment and management of emergency protection controls such as emergency shutdown of the IT system, backup for power and lighting, controls for temperature and humidity, and protection against fire and water damage.

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

- NIST SP 800-12 provides guidance on security policies and procedures [39].
- NIST SP 800-46 provides guidance on security in telecommuting and broadband communications [52].

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

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

ICS Specific Recommendations and Guidance

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

Gaining physical access to a control room or control system components often implies gaining logical access to the process control system as well.

Likewise, having logical access to systems such as main servers and control room computers allows an adversary to exercise control over the physical process. If computers are readily accessible, and they have removable media drives (e.g., floppy disks, compact discs, etc.) or USB ports, the drives can be fitted with locks or removed from the computers and USB ports disabled.

Depending on security needs and risks, it might also be prudent to disable or physically protect power buttons to prevent unauthorized use. For maximum security, servers should be placed in locked areas and authentication mechanisms (such as keys) protected. In addition, the network devices on the ICS network, including switches, routers, network jacks, servers, workstations, and controllers, should be located in a secured area that can only be accessed by authorized personnel. The secured area should also be compatible with the environmental requirements of the devices.

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

Protection of Physical Locations

Classic physical security considerations typically refer to a ringed architecture of layered security measures. Creating several physical barriers, both active and passive, around buildings, facilities, rooms, equipment, or other informational assets, establishes these physical security perimeters. Physical security controls meant to protect physical locations include fences, anti-vehicle ditches, earthen mounds, walls, reinforced barricades, gates, or other measures. Most organizations include this layered model by preventing access to the plant first by the use of fences, guard shacks, gates, and locked doors.

Access Control
Access control systems should ensure that only authorized people have access to controlled spaces. An access control system should be flexible. The need for access may be based on time (day vs. night shift), level of training, employment status, work assignment, plant status, and a myriad of other factors. A system must be able to verify that persons being granted access are who they say they are (usually using something the person has, such as an access card; something they know, such as a personal identification number (PIN); or something they are, using abiometric). Access control should be highly reliable yet not interfere with the routine or emergency duties of plant personnel. Integration of access control into the process system allows a view into not only security access, but also physical and personnel asset tracking, dramatically accelerating response time in emergencies, helping to direct individuals to safe locations, and improving overall productivity.

Within an area, access to network and computer cabinets should be limited to only those who have a need, such as network technicians and engineers, or computer maintenance staff. Equipment cabinets should be locked and wiring should be neat and within cabinets. Consider keeping all computers in secure racks and using peripheral extender technology to connect human-machine interfaces to the racked computers.

Access Monitoring Systems
Access monitoring systems include still and video cameras, sensors, and various types of identification systems. Examples of these systems include cameras that monitor parking lots, convenience stores, or airline security. These devices do not specifically prevent access to a particular location; rather, they store and record either the physical presence or the lack of physical presence of individuals, vehicles, animals, or other physical entities. Adequate lighting should be provided based on the type of access monitoring device deployed.

Access Limiting Systems
Access limiting systems may employ a combination of devices to physically control or prevent access to protected resources. Access limiting systems include both active and passive security devices such as fences, doors, safes, gates, and guards. They are often coupled with Identification and monitoring systems to provide role-based access for specific individuals or groups of individuals.

People and Asset Tracking
Locating people and vehicles in a large installation is important for safety reasons, and it is increasingly important for security reasons as well. Asset location technologies can be used to track the movements of people and vehicles within the plant, to ensure that they stay in authorized areas, to identify personnel needing assistance, and to support emergency response.

Environmental Factors
In addressing the security needs of the system and data, it is important to consider environmental factors. For example, if a site is dusty, systems should be placed in a filtered environment. This is particularly important if the dust is likely to be conductive or magnetic, as in the case of sites that process coal or iron. If vibration is likely to be a problem, systems should be mounted on rubber bushings to prevent disk crashes and wiring connection problems. In addition, the environments containing systems and media (e.g., backup tapes, floppy disks) should have stable temperature and humidity. An alarm to the process control system should be generated when environmental specifications such as temperature and humidity are exceeded.

Environmental Control Systems
Heating, ventilation, and air conditioning (HVAC) systems for control rooms must support plant personnel during normal operation and emergency situations, which could include the release of toxic substances. Fire systems must be carefully designed to avoid causing more harm than good (e.g., to avoid mixing water with incompatible products). HVAC and fire systems have significantly increased roles in security that arise from the interdependence of process control and security. For example, fire prevention and HVAC systems that support industrial control computers need to be protected against cyber incidents.

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

6.2.2.1 Control Center/Control Room

ICS Specific Recommendations and Guidance
Providing physical security for the control center/control room is essential to reduce the potential of many threats. Control centers/control rooms frequently have consoles continuously logged onto the primary control server, where speed of response and continual view of the plant is of utmost importance. These areas will often contain the servers themselves, other critical computer nodes, and sometimes plant controllers. It is essential to limit access to these areas using authentication methods such as smart or magnetic identity cards or biometric readers. In extreme cases, it may be considered necessary to make the control center/control room blast-proof, or to provide an offsite emergency control center/control room so that control can be maintained if the primary control center/control room becomes uninhabitable.

6.2.2.2 Portable Devices
ICS Specific Recommendations and Guidance
Computers and computerized devices used for ICS functions (such as PLC programming) should never leave the ICS area. Laptops and portable engineering workstations should be tightly secured and never used outside the ICS network. Antivirus and patch management should be kept current.

6.2.2.3 Cabling
ICS Specific Recommendations and Guidance
Cabling for the control network should be addressed in the cyber security plan. Unshielded twisted pair communications cable, while acceptable for the office environment, is generally not suitable for the plant environment due to its susceptibility to interference from magnetic fields, radio waves, temperature extremes, moisture, dust, and vibration. Industrial RJ-45 connectors should be used in place of other types of twisted pair connectors to provide protection against moisture, dust and vibration.

Fiber-optic cable and coaxial cable are often better network cabling choices for the control network since they are immune to many of the typical environmental conditions including electrical and radio frequency interference found in an industrial control environment. Cable and connectors should be color-coded and labeled so that the ICS and IT networks are clearly delineated and potential for an inadvertent cross-connect is reduced.

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

6.2.3 Contingency Planning

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

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

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

- NIST SP 800-12 provides guidance on security policies and procedures [39].
- NIST SP 800-34 provides guidance on contingency planning [53].

ICS Specific Recommendations and Guidance

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

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

6.2.3.1 Business Continuity Planning

Business continuity planning addresses the overall issue of maintaining or re-establishing production in the case of an interruption. These interruptions may take the form of a natural disaster (e.g., hurricane, tornado, earthquake, flood), an unintentional man-made event (e.g., accidental equipment damage, fire or explosion, operator error), an intentional man-made event (e.g., attack by bomb, firearm or vandalism, attacker or virus), or an equipment failure. From a potential outage perspective, this may involve typical time spans of days, weeks, or months to recover from a natural disaster, or minutes or hours to recover from a malware infection or a mechanical/electrical failure.

Since there is often a separate discipline that deals with reliability and electrical/mechanical maintenance, some organizations choose to define business continuity in a way that excludes these sources of failure. Since business continuity also deals primarily with the long-term implications of production outages, some organizations also choose to place a minimum interruption limit on the risks to be considered.

For the purposes of ICS cyber security, it is recommended that neither of these constraints be made. Long-term outages (disaster recovery) and short-term outages (operational recovery) should both be considered.

Because some of these potential interruptions involve man-made events, it is also important to work collaboratively with the physical security organization to understand the relative risks of these events and the physical security countermeasures that are in place to prevent them. It is also important for the physical security organization to understand which areas of a production site house data acquisition and control systems that might have higher-level risks.

Before creating a business continuity plan (BCP) to deal with potential outages, it is important to specify the recovery objectives for the various systems and subsystems involved based on typical business needs. There are two distinct types of objectives: system recovery and data recovery. System recovery involves the recovery of all communication links and processing capabilities, and it is usually specified in terms of a Recovery Time Objective (RTO). This is defined as the time required to recover all communication links and processing capabilities. Data recovery involves the recovery of data describing production or product conditions in the past and is usually specified in terms of a Recovery Point Objective (RPO). This is defined as the longest period of time for which an absence of data can be tolerated.

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

Due to the potential cost and importance of these contingency plans, they should be reviewed with the managers responsible for business continuity planning to verify that they are justified. Once the recovery procedures are documented, a schedule should be developed to test part or all of the recovery procedures. Particular attention must be paid to the verification of backups of system configuration data and product or production data. Not only should these be tested when they are produced, but the procedures followed for their storage should also be reviewed periodically to verify that the backups are kept in environmental conditions that will not render them unusable and that they are kept in a secure location, so they can be quickly obtained by authorized individuals when needed.

6.2.3.2 Disaster Recovery Planning

ICS Specific Recommendations and Guidance

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

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

The plan should also indicate requirements for the timely replacement of components in the case of an emergency. If possible, replacements for hard-to-obtain critical components should be kept in inventory.

The security plan should define a comprehensive backup and restore policy. In formulating this policy, the following should be considered:

1. The speed at which data or the system must be restored. This requirement may justify the need for a redundant system, spare offline computer, or valid file system backups.
2. The frequency at which critical data and configurations are changing. This will dictate the frequency and completeness of backups.
3. The safe onsite and offsite storage of full and incremental backups.
4. The safe storage of installation media, license keys, and configuration information.
5. Identification of individuals responsible for performing, testing, storing, and restoring backups

6.2.4 Configuration Management

Configuration management policy and procedures are used to control modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation. The security controls that fall within the NIST SP 800-53 Configuration Management (CM) family provide policy and procedures for establishing baseline controls for information systems.

Controls are also specified for maintaining, monitoring, and documenting configuration control changes. There should be restricted access to configuration settings, and security settings of IT products should be set to the most restrictive mode consistent with ICS operational requirements.

Supplemental guidance for the CM controls can be found in the following documents:
- NIST SP 800-12 provides guidance on security policies and procedures [39].
- NIST SP 800-70 provides guidance on configuration settings for IT products [25].

ICS Specific Recommendations and Guidance
A formal change management procedure is used to insure that all modifications to an ICS network meet he same security requirements as the original components identified in the asset evaluation and the associated risk assessment and mitigation plans. Risk assessment should be performed on all changes to the ICS network that could affect security, including configuration changes, the addition of network components, and installation of software. Changes to policies and procedures may also be required. The current ICS network configuration must always be known and documented.

6.2.5 Maintenance
The security controls that fall within the NIST SP 800-53 Maintenance (MA) family provide policy and procedure for performing routine and preventative maintenance on the components of an information system. This includes the usage of maintenance tools (both local and remote) and management of maintenance personnel.

Supplemental guidance for the MA controls can be found in the following documents:
- NIST SP 800-12 provides guidance on security policies and procedures [39].
- NIST SP 800-63 provides guidance on electronic authentication for remote maintenance [54].

6.2.6 System and Information Integrity
Maintaining system and information integrity assures that sensitive data has not been modified or deleted in an unauthorized and undetected manner. The security controls that fall within the NIST SP 800-53 System and Information Integrity (SI) family provide policies and procedures for identifying, reporting, and correcting information system flaws. Controls exist for malicious code detection, spam and spyware protection, and intrusion detection, although they may not be appropriate for all ICS applications.

Also provided are controls for receiving security alerts and advisories, and the verification of security functions on the information system. In addition, there are controls within this family to detect and protect against unauthorized changes to software and data, provide restrictions to data input and output, and check for the accuracy, completeness, and validity of data as well as handle error conditions, although they may not be appropriate for all ICS applications.

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

- NIST SP 800-12 provides guidance on security policies and procedures [39].
- NIST SP 800-40 provides guidance on security patch installation [40].
- NIST SP 800-31 provides guidance on intrusion detection [55].
- NIST SP 800-94 provides guidance on Intrusion Detection and Prevention (IDP) Systems [56].

ICS Specific Recommendations and Guidance
Controls exist for malicious code detection, spam and spyware protection, and intrusion detection, although they may not be appropriate for all ICS applications.

6.2.6.1 Malicious Code Detection
Anti-virus products evaluate files on a computer's storage devices against an inventory of known virus signature files. If one of the files on a computer matches the profile of a known virus, the virus is removed through a disinfection process so it cannot infect other local files or communicate across a network to infect other files. Anti-virus software can be deployed on workstations, servers, firewalls and handheld devices.

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

While antivirus tools are common security practice in IT computer systems, their use with ICS may require adopting special practices including compatibility checks, change management issues, and performance impact metrics. These special practices should be utilized whenever new signatures or new versions of antivirus software are installed.

Major ICS vendors recommend and even support the use of particular antivirus tools. In some cases, control system vendors may have performed regression testing across their product line for supported versions of a particular antivirus tool and also provide associated installation and configuration documentation. There is also an effort to develop a general set of guidelines and test procedures focused on ICS performance impacts to fill the gaps where ICS and antivirus vendor guidance is not available [57].

Generally:
Windows, Unix, Intel chip set computers used as consoles, engineering workstations, data historians, pseudo-DCSs (PLC supervisors) such as Wonderware, HMIs, and general purpose SCADA and backup servers can be secured just like commercial IT equipment: install push- or auto-updated antivirus and patch management software with updates distributed via an anti-virus server and patch management server located inside the process control network and auto-updated from the IT network

Follow vendor recommendations on all other servers and computers (DCS, PLC, instruments) that have time-dependent code, modified or extended the operating system or any other change that makes it different from any standard PC that one could buy at an office supply or computer store. Expect the vendor to make periodic maintenance releases that include security patches.

6.2.6.2 Intrusion Detection and Prevention

Intrusion detection systems (IDS) monitor events on a network, such as traffic patterns, or a system, such as log entries or file accesses, so that they can identify an intruder breaking into or attempting to break into a system [58]. IDSs ensure that unusual activity such as new open ports, unusual traffic patterns, or changes to critical operating system files is brought to the attention of the appropriate security personnel.

The two most commonly used types of IDS are:

Network-Based IDS. These systems monitor network traffic and generate alarms when they identify traffic that they deem to be an attack.

Host-Based IDS. This software monitors one or more types of characteristics of a system, such as application log file entries, system configuration changes, and access to sensitive data on a system and responds with an alarm or countermeasure when a user attempts to breach security.

ICS Specific Recommendations and Guidance

An effective IDS deployment typically involves both host-based and network-based IDSs. In the ICS environment, network-based IDSs are most often deployed between the control network and the corporate network in conjunction with a firewall; host-based IDSs are most often deployed on the computers that use general-purpose OSs or applications such as HMIs, SCADA servers, and engineering workstations.

Properly configured, an IDS can greatly enhance the security management team's ability to detect attacks entering or leaving the system, thereby improving security. They can also potentially improve a control network's efficiency by detecting non-essential traffic on the network. However, even when IDSs are implemented, security staff can primarily recognize individual attacks, as opposed to organized patterns of attacks over time. Additionally, care should be given to not confuse unusual ICS activity, such as during transient conditions, as an attack.

Current IDS and IPS products are effective in detecting and preventing well-known Internet attacks, but until recently they have not addressed ICS protocol attacks. IDS and IPS vendors are beginning to develop and incorporate attack signatures for various ICS protocols such as Modbus, DNP, and ICCP. [59] [60] Appendix D provides some additional information on emerging IDS capabilities.

6.2.6.3 Patch Management

ICS Specific Recommendations and Guidance

Applying patches to OS components creates another situation where significant care should be exercised in the ICS environment. Patches should be adequately tested to determine the acceptability of side effects. Regression testing is advised. It is not uncommon for patches to have an adverse effect on other software. A patch may remove a vulnerability, but it can also introduce a greater risk from a production or safety perspective. Patching the vulnerability may also change the way the OS or application works with control applications, causing the control application to lose some of its functionality. Once the decision is made to deploy a patch, there are other tools that automate this process from a centralized server and with confirmation that the patch has been deployed correctly. Consider separating the automated process for ICS patch management from the automated process for non-ICS applications. Patching should be scheduled to occur during planned ICS outages.

6.2.7 Media Protection

The security controls that fall within the NIST SP 800-53 Media Protection (MP) family provide policies and procedures for limiting the access to media to authorized users.

Controls also exist for labeling media for distribution and handling requirements, as well as storage, transport, sanitization (removal of information from digital media), destruction, and disposal of the media.

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

- NIST SP 800-12 provides guidance on security policies and procedures [39].
- NIST SP 800-88 provides guidance on appropriate sanitization equipment, techniques, and procedures [80].

ICS Specific Recommendations and Guidance

Media assets include removable media and devices such floppy disks, CDs, DVDs and USB memory sticks, as well as printed reports and documents. Physical security controls should address specific requirements for the safe maintenance of these assets and provide specific guidance for transporting, handling, and erasing or destroying these assets.

Security requirements could include safe storage from loss, fire, theft, unintentional distribution, or environmental damage. If an adversary gains access to backup media associated with an ICS, it could provide valuable data for launching an attack.

Recovering an authentication file from the backups might allow an adversary to run password cracking tools and extract usable passwords. In addition, the backups typically contain machine names, IP addresses, software version numbers, usernames, and other data useful in planning an attack.

The use of any unauthorized CDs, DVDs, floppy disks, USB memory sticks, or similar removable media on any node that is part of or connected to the ICS should not be permitted; this can prevent the introduction of malware or the inadvertent loss or theft of data. Where the system components use unmodified industry standard protocols, mechanized policy management software can be used to enforce media protection policy.

6.2.8 Incident Response

An incident response plan is documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of incidents against an organization's information systems. Response should be measured first and foremost against the "service being provided", not just the system that was compromised. If an incident is discovered, there should be a quick risk assessment performed to evaluate the effect of both the attack and the options to respond.

For example, one possible response option is to physically isolate the system under attack. However, this may have such a dire impact on the service that it is dismissed as not viable.

The security controls that fall within the NIST SP 800-53 Incident Response (IR) family provide policies and procedures for incident response monitoring, handling, and reporting. The handling of a security incident includes preparation, detection and analysis, containment, eradication, and recovery. Controls also cover incident response training for personnel and testing the incident response capability for an information system.

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

- NIST SP 800-12 provides guidance on security policies and procedures [39].
- NIST SP 800-61 provides guidance on incident handling and reporting [61].
- NIST SP 800-83 provides guidance on malware incident prevention and handling [62].

ICS Specific Recommendations and Guidance

Regardless of the steps taken to protect an ICS, it is always possible that it may be compromised by an intentional or unintentional incident. The following symptoms can arise from normal network problems, but when several symptoms start to appear, a pattern may indicate the ICS is under attack and may be worth investigating further. If the adversary is skilled, it may not be very obvious that an attack is underway.

The symptoms of an incident could include any of the following:

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

To minimize the effects of these intrusions, it is necessary to plan a response. Incident response planning defines procedures to be followed when an intrusion occurs. NIST SP 800-61, *Computer Security Incident Handling Guide*, provides guidance on incident response planning, which might include the following items:

Classification of Incidents

The various types of ICS incidents should be identified and classified as to potential impact and likelihood so that a proper response can be formulated for each potential incident.

Response Actions

There are several responses that can be taken in the event of an incident. These range from doing nothing to full system shutdown (although full shutdown is highly unlikely for an ICS). The response taken will depend on the type of incident and its effect on the ICS system and the physical process being controlled. A written plan documenting the types of incidents and the response to each type should be prepared. This will provide guidance during times when there might be confusion or stress due to the incident. This plan should include step-by-step actions to be taken by the various organizations. If there are reporting requirements, these should be noted as well as where the report should be made and phone numbers to reduce reporting confusion.

Recovery Actions
The results of the intrusion might be minor or could cause many problems in the ICS. Prior analysis should be conducted to determine the sensitivity of the physical system being controlled to failure modes in the ICS. In each case, step-by-step recovery actions should be documented so that the system can be returned to normal operations as quickly and safely as possible.

During the preparation of the incident response plan, input should be obtained from the various stakeholders including operations, management, organized labor, legal, and safety. These stakeholders should also review and approve the plan.

6.2.9 Awareness and Training
The security controls that fall within the NIST SP 800-53 Awareness and Training (AT) family provide policy and procedures for ensuring that all users of an information system are provided basic information system security awareness and training materials before authorization to access the system is granted. Personnel training must be monitored and documented.

Supplemental guidance for the AT controls can be found in the following documents:
- NIST SP 800-12 provides guidance on security policies and procedures [39].
- NIST SP 800-16 provides guidance on security training requirements
- NIST SP 800-50 provides guidance on security awareness training [63].

ICS Specific Recommendations and Guidance
For the ICS environment, this must include control system-specific information security awareness and training for specific ICS applications. In addition, an organization must identify, document, and train all personnel with significant information system roles and responsibilities. Awareness and training must cover the physical process being controlled as well as the ICS.

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

Implementing an ICS security program may bring changes to the way in which personnel access computer programs, applications, and the computer desktop itself. Organizations should design effective training programs and communication vehicles to help employees understand why new access and control methods are required, ideas they can use to reduce risks and the impact on the organization if control methods are not incorporated.

Training programs also demonstrate management’s commitment to, and the value of, a cyber-security program. Feedback from staff exposed to this type of training can be a valuable source of input for refining the charter and scope of the security program.

6.3 Technical Controls

Technical controls are the security countermeasures for an ICS that are primarily implemented and executed by the system through mechanisms contained in the hardware, software, or firmware components of the system. As discussed in detail in the following subsections, NIST SP 800-53 defines four families of controls within the Technical controls class:

Identification and Authentication (IA): the process of verifying the identity of a user, process, or device, as a prerequisite for granting access to resources in an IT system.

Access Control (AC): the process of granting or denying specific requests for obtaining and using information and related information processing services for physical access to areas within the information system environment.

Audit and Accountability (AU): independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

System and Communications Protection (SC): mechanisms for protecting both system and data transmission components.

These technical controls are discussed in more detail in the sections to follow. Initial ICS specific recommendations and guidance, if available, will be provided in an outlined box for each section. Additional ICS specific guidance pertaining to technical controls can be found in ISA TR99.00.01 [34] and the EPRI report: *Supervisory Control and Data Acquisition (SCADA) Systems Security Guide* [64].

6.3.1 Identification and Authentication

Authentication describes the process of positively identifying potential network users, hosts, applications, services, and resources using a combination of identification factors or credentials. The result of this authentication process then becomes the basis for permitting or denying further actions (e.g., when an automatic teller machine asks for a PIN). Based on the authentication determination, the system may or may not allow the potential user access to its resources. Authorization is the process of determining who and what should be allowed to have access to a particular resource; access control is the mechanism for enforcing authorization. Access control is described in Section 6.3.2.

There are several possible factors for determining the authenticity of a person, device, or system, including something you know, something you have or something you are. For example, authentication could be based on something known (e.g., PIN number or password), something possessed (e.g., key, dongle, smart card), a biological characteristic such as a fingerprint or retinal signature, a location (e.g., Global Positioning System [GPS] location access), the time a request is made, or a combination of these attributes. In general, the more factors that are used in the authentication process, the more robust the process will be. When two or more factors are used, the process is known generically as *multi-factor authentication*.

The security controls that fall within the NIST SP 800-53 Identification and Authentication (IA) family provide policy and guidance for the identification and authentication of users of and devices within the information system.

These include controls to manage identifiers and authenticators within each technology used (e.g., tokens, certificates, biometrics, passwords, key cards).

Supplemental guidance for the IA controls can be found in the following documents:
- NIST SP 800-12 provides guidance on security policies and procedures [39].
- NIST SP 800-63 provides guidance on remote electronic authentication [54].
- NIST SP 800-73 provides guidance on interfaces for personal identity verification [50].
- NIST SP 800-76 provides guidance on biometrics for personal identity verification [51].

ICS Specific Recommendations and Guidance
Computer systems in ICS environments typically rely on traditional passwords for authentication. Control system suppliers often supply systems with default passwords. These passwords are often easy to guess or are changed infrequently, which creates additional security risks. In addition, protocols currently used in ICS environments generally have inadequate or no network service authentication. There are now several forms of authentication available in addition to traditional password techniques being used with ICS. Some of these, including password authentication, are presented in the following sections with discussions regarding their use with ICS.

6.3.1.1 Password Authentication
Password authentication technologies determine authenticity based on testing for something the device or human requesting access should know, such as a PIN number or password. Password authentication schemes are thought of as the simplest and most common forms of authentication.

Password vulnerabilities can be reduced by using an active password checker that prohibits weak, recently used, or commonly used passwords. Another weakness is the ease of third-party eavesdropping. Passwords typed at a keypad or keyboard are easily observed or recorded, especially in areas where adversaries could plant tiny wireless cameras or keystroke loggers. Network service authentication often transmits passwords as plaintext (unencrypted), allowing any network capture tool to expose the passwords.

ICS Specific Recommendations and Guidance
One problem with passwords unique to the ICS environment is that a user's ability to recall and enter a password may be impacted by the stress of the moment. During a major crisis when human intervention is critically required to control the process, an operator may panic and have difficulty remembering or entering the password and either be locked out completely or be delayed in responding to the event.

Biometric identifies may have similar drawbacks. It is recommended not to use password authorizations on these critical control systems but instead to use other compensating controls, such as rigorous physical security controls.

Some ICS operating systems make setting secure passwords difficult, as the password size is very small and the system allows only group passwords at each level of access, not individual passwords. Some industrial (and Internet) protocols transmit passwords in plaintext, making them susceptible to interception. In cases where this practice cannot be avoided, it is important that users have different (and unrelated) passwords for use with encrypted and non-encrypted protocols.

Password Recommendations
The following are general recommendations and considerations with regards to the use of passwords. Specific recommendations are presented in ISA-TR99.00.02-2004 [27].

- The length, strength, and complexity of passwords should balance security and operational ease of access within the capabilities of the software and underlying OS.
- Passwords should have appropriate length and entropy characterization for the security required. In particular, they should not be able to be found in a dictionary or contain predictable sequences of numbers or letters.
- Passwords should be used with care on operator interface devices such as control consoles on critical processes. Using passwords on these consoles could introduce potential safety issues if operators are locked out or delayed access during critical events.
- The keeper of master passwords should be a trusted employee, available during emergencies. A copy of the master passwords may want to be stored in a very secure location.
- The passwords of privileged users (such as network technicians, electrical or electronics technicians and management, and network designers/operators) should be most secure and be changed frequently. Authority to change master passwords should be limited to trusted employees. A password audit record, especially for master passwords, should be maintained separately from the control system.
- In environments with a high risk of interception or intrusion (such as remote operator interfaces in a facility that lacks local physical security access controls), organizations should consider supplementing password authentication with other forms of authentication such as challenge/response or two-factor authentication using biometric or physical tokens.
- For user authentication purposes, password use is common and generally acceptable for users logging directly into a local device or computer. Passwords should not be sent across any network unless protected by some form of FIPS-approved encryption or salted cryptographic hash specifically designed to prevent replay attacks. It is assumed that the device used to enter a password is connected to the network in a secure manner.
- For network service authentication purposes, passwords should be avoided if possible. There are more secure alternatives available, such as challenge/response or public key authentication.

6.3.1.2 Challenge/Response Authentication

Challenge/response authentication requires that both the service requester and service provider know a “secret” code in advance. When service is requested, the service provider sends a random number or string as a challenge to the service requester. The service requester uses the secret code to generate a unique response for the service provider. If the response is as expected, it proves that the service requester has access to the “secret” without ever exposing the secret on the network.

Challenge/response authentication addresses the security vulnerabilities of traditional password authentication. When passwords (hashed or plain) are sent across a network, a portion of the actual “secret itself is being sent. Authentication is performed by giving the secret to the remote device.

6.3.1.3 Physical Token Authentication

Physical or token authentication is similar to password authentication, except that these technologies determine authenticity by testing for secret code or key produced by a device or token the person requesting access has in their possession, such as security tokens or smart cards. Increasingly, private keys are being embedded in physical devices such as USB dongles.

Some tokens support single-factor authentication only, so that simply having possession of the token is sufficient to be authenticated. Others support two-factor authentication that requires knowledge of a PIN or password in addition to possessing the token.

The primary vulnerability that token authentication addresses is easily duplicating a secret code or sharing it with others. It eliminates the all-too-common scenario of a password to a “secure” system being left on the wall next to a PC or operator station.

The security token cannot be duplicated without special access to equipment and supplies. A second benefit is that the secret within a physical token can be very large, physically secure, and randomly generated. Because it is embedded in metal or silicon, it does not have the same risks that manually entered passwords do. If a security token is lost or stolen, the authorized user loses access, unlike traditional passwords that can be lost or stolen without notice.

Common forms of physical/token authentication include:

- Traditional physical lock and keys
- Security cards (e.g., magnetic, smart chip, optical coding)
- Radio frequency devices in the form of cards, key fobs, or mounted tags
- Dongles with secure encryption keys that attach to the USB, serial, or parallel ports of computers
- One-time authentication code generators (e.g., key fobs)

For single-factor authentication, the largest weakness is that physically holding the token means access is granted (e.g., anyone finding a set of lost keys now has access to whatever they open). Physical/token authentication is more secure when combined with a second form of authentication, such as a memorized PIN used along with the token.

ICS Specific Recommendations and Guidance

Two-factor authentication is an accepted good practice for access to ICS applications from outside the ICS firewall.

Physical/token authentication has the potential for a strong role in ICS environments.

An access card or other token can be an effective form of authentication for computer access, as long as the computer is in a secure area (e.g., once the operator has gained access to the room with appropriate secondary authentication, the card alone can be used to enable control actions).

6.3.1.4 Biometric Authentication

Biometric authentication technologies determine authenticity by determining presumably unique biological characteristics of the human requesting access. Usable biometric features include finger minutiae, facial geometry, retinal and iris signatures, voice patterns, typing patterns, and hand geometry.

Like physical tokens and smart cards, biometric authentication enhances software-only solutions, such as password authentication, by offering an additional authentication factor and removing the human element in memorizing complex secrets. In addition, since biometric characteristics are unique to a given individual, biometric authentication addresses the issues of lost or stolen physical tokens and smart cards.

Noted issues with biometric authentication include:

- Distinguishing a real object from a fake (e.g., how to distinguish a real human finger from a silicon-rubber cast of one or a real human voice from a recorded one).
- Generating type-I and type-II errors (the probability of rejecting a valid biometric image, and the probability of accepting an invalid biometric image, respectively). Biometric authentication devices should be configured to the lowest crossover between these two probabilities, also known as the crossover error rate.
- Handling environmental factors such as temperature and humidity to which some biometric devices are sensitive.
- Addressing industrial applications where employees may have on safety glasses and/or gloves and industrial chemicals may impact biometric scanners.
- Retraining biometric scanners that occasionally “drift” over time. Human biometric traits may also shift over time, necessitating periodic scanner retraining.
- Requiring face-to-face technical support and verification for device training, unlike a password that can be given over a phone or an access card that can be handed out by a receptionist.
- Denying needed access to the control system because of a temporary inability of the sensing device to acknowledge a legitimate user.
- Being socially acceptable. Users consider some biometric authentication devices more acceptable than others. For example, retinal scans may be considered very low on the scale of acceptability, while thumb print scanners may be considered high on the scale of acceptability. Users of biometric authentication devices will need to take social acceptability for their target group into consideration when selecting among various biometric authentication technologies.

ICS Specific Recommendations and Guidance

Biometric devices make a useful secondary check versus other forms of authentication that can become lost or borrowed. Using biometric authentication in combination with token-based access control or badge-operated employee time clocks increases the security level. A possible application is in a control room that is environmentally controlled and physically secured [34].

6.3.2 Access Control

The security controls that fall within the NIST SP 800-53 Access Control (AC) family provide policies and procedures for specifying the use of system resources by only authorized users, programs, processes, or other systems. This family specifies controls for managing information system accounts, including establishment, activating, modifying, reviewing, disabling, and removing accounts.

Controls cover access and flow enforcement issues such as separation of duties, least privilege, unsuccessful login attempts, system use notification, previous logon notification, concurrent session control, session lock, and session termination. There are also controls to address the use of portable and remote devices and personally owned information systems to access the information system as well as the use of remote access capabilities and the implementation of wireless technologies.

Access can take several forms, including viewing, using, and altering specific data or device functions. Supplemental guidance for the AC controls can be found in the following documents:

- NIST SP 800-12 provides guidance on security policies and procedures [39].
- NIST SP 800-63 provides guidance on remote electronic authentication [54].
- NIST SP 800-48 provides guidance on wireless network security with particular emphasis on the IEEE 802.11b and Bluetooth standards [65].
- NIST SP 800-97 provides guidance on IEEE 802.11i wireless network security [66].
- FIPS 201 requirements for the personal identity verification of federal employees and contractors [67].
- NIST SP 800-96 provides guidance on PIV card to reader interoperability [68].
- NIST SP 800-73 provides guidance on interfaces for personal identity verification [50].
- NIST SP 800-76 provides guidance on biometrics for personal identity verification [51].
- NIST SP 800-78 provides guidance on cryptographic algorithms and key sizes for personal identity verification [69].

If the new federal Personal Identity Verification (PIV) is used as an identification token, the access control system should conform to the requirements of FIPS 201 and NIST SP 800-73 and employ either cryptographic verification or biometric verification. When token-based access control employs cryptographic verification, the access control system should conform to the requirements of NIST SP 800-78.

When token-based access control employs biometric verification, the access control system should conform to the requirements of NIST SP 800-76. Access control technologies are filter and blocking technologies designed to direct and regulate the flow of information between devices or systems once authorization has been determined. The following sections present several access control technologies and their use with ICS.

6.3.2.1 Role-based Access Control (RBAC)

RBAC is a technology that has the potential to reduce the complexity and cost of security administration in networks with large numbers of intelligent devices. Under RBAC, security administration is simplified through the use of roles, hierarchies, and constraints to organize user access levels. RBAC reduces costs within an organization because it accepts that employees change roles and responsibilities more frequently than the duties within roles and responsibilities.

ICS Specific Recommendations and Guidance

RBAC can be used to provide a uniform means to manage access to ICS devices while reducing the cost of maintaining individual device access levels and minimizing errors. RBAC should be used to restrict ICS user privileges to only those that are required to perform each person's job (i.e., configuring each role based on the principle of least privilege).

6.3.2.2 Web Servers

Web and Internet technologies are being added to a wide variety of ICS products because they make information more accessible and products more user-friendly and easier to configure remotely. However, they may also add cyber risks and create new security vulnerabilities that need to be addressed.

ICS Specific Recommendations and Guidance

SCADA and historian software vendors typically provide Web servers as a product option so that users outside the control room can access ICS information. In many cases, software components such as ActiveX controls or Java applets must be installed or downloaded onto each client machine accessing the Web server. Some products, such as PLCs and other control devices, are available with embedded Web, FTP, and e-mail servers to make them easier to configure remotely and allow them to generate e-mail notifications and reports when certain conditions occur.

6.3.2.3 Virtual Local Area Network (VLAN)

VLANs divide physical networks into smaller logical networks to increase performance, improve manageability, and simplify network design. VLANs are achieved through configuration of Ethernet switches. Each VLAN consists of a single broadcast domain that isolates traffic from other VLANs. Just as replacing hubs with switches reduces collisions, using VLANs limits the broadcast traffic, as well as allowing logical subnets to span multiple physical locations.

There are two categories of VLANs:

- Static, often referred to as port-based, where switch ports are assigned to a VLAN so that it is transparent to the end user.
- Dynamic, where an end device negotiates VLAN characteristics with the switch or determines the VLAN based on the IP or hardware addresses.

Although more than one IP subnet may coexist on the same VLAN, the general recommendation is to use a one-to-one relationship between subnets and VLANs. This practice requires the use of a router or multi-layer switch to join multiple VLANs. Many routers and firewalls support tagged frames so that a single physical interface can be used to route between multiple logical networks.

VLANs are not typically deployed to address host or network vulnerabilities in the way that firewalls or IDSs are. However, when properly configured, VLANs do allow switches to enforce security policies and segregate traffic at the Ethernet layer.

Properly segmented networks can also mitigate the risks of broadcast storms that may result from port scanning or worm activity.

Switches have been susceptible to attacks such as MAC spoofing, table overflows, and attacks against the spanning tree protocols, depending on the device and its configuration. VLAN hopping, the ability for an attack to inject frames to unauthorized ports has been demonstrated using switch spoofing or double- encapsulated frames.

These attacks cannot be conducted remotely and require local physical access to the switch. A variety of features such as MAC address filtering, port-based authentication using IEEE 802.1x, and specific vendor best practices can be used to mitigate these attacks, depending on the device and implementation.

ICS Specific Recommendations and Guidance
VLANs have been effectively deployed in ICS networks, with each automation cell assigned to a single VLAN to limit unnecessary traffic flooding and allow network devices on the same VLAN to span multiple switches [34].

6.3.2.5 Wireless

The use of wireless within an ICS is a risk-based decision that has to be determined by the organization. Generally, wireless LANs should only be deployed where health, safety, environmental, and financial implications are low. NIST SP 800-48 and SP 800-97 provide guidance on wireless network security.

ICS Specific Recommendations and Guidance

- Prior to installation, a wireless survey should be performed to determine antenna location and strength to minimize exposure of the wireless network. The survey should take into account the fact that attackers can use powerful directional antennas, which extend the effective range of a wireless LAN beyond the expected standard range.
- Wireless users' access should utilize IEEE 802.1x authentication using a secure authentication protocol (e.g., Extensible Authentication Protocol [EAP] with TLS [EAP-TLS]) that authenticates users via either user certificates or a Remote Authentication Dial In User Service (RADIUS) server.
- The wireless access points and data servers for wireless worker devices should be located on an isolated network with documented and minimal (single if possible) connections to the ICS network topology.
- Wireless access points should be configured to have a unique service set identifier (SSID), disable SSID broadcast, and enable MAC filtering at a minimum.
- Wireless devices, if being utilized in a Microsoft Windows ICS network, should be configured into a separate organizational unit of the Windows domain.
- Wireless device communications should be encrypted and integrity-protected. The encryption must not degrade the operational performance of the end device. Encryption at OSI Layer 2 should be considered, rather than at Layer 3 to reduce encryption latency. The use of hardware accelerators to perform cryptographic functions should also be considered.

For mesh networks, consider the use of broadcast key versus public key management implemented at OSI Layer 2 to maximize performance. Asymmetric cryptography should be used to perform Administrative functions and Symmetric encryption should be used to secure each data stream as well as network control traffic. An adaptive routing protocol should be considered if the devices are to be used for wireless mobility. The convergence time of the network should be as fast as possible supporting rapid network recovery in the event of a failure or power loss. It should also be noted that deployment of a mesh network may provide fault tolerance thru alternate route selection and pre-emptive fail-over of the network

The ISA-SP10019 Committee is working to establish standards, recommended practices, technical reports, and related information that will define procedures for implementing wireless systems in the automation and control environment with a focus on the field level. Guidance is directed towards those responsible for the complete life cycle including the designing, implementing, on-going maintenance, scalability or managing manufacturing and control systems, and shall apply to users, system integrators, practitioners, and control systems manufacturers and vendors.

6.3.3 Audit and Accountability

An audit is an independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. The security controls that fall within the NIST SP 800-53 Audit and Accountability (AU) family provide policies and procedures for generating audit records, their content, capacity, and retention requirements.

The controls also provide safeguards to react to problems such as an audit failure or audit log capacity being reached. Audit data should be protected from modification and be designed with non-repudiation capability.

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

- NIST SP 800-12 provides guidance on security policies and procedures [39].
- NIST SP 800-61 provides guidance on computer security incident handling and audit log retention [61].
- NIST SP 800-92 provides guidance on log management (including audit logs) [70]

ICS Specific Recommendations and Guidance

It is necessary to determine that the system is performing as intended. Periodic audits of the ICS should be performed to validate the following items:

- The security controls present during system validation testing are still installed and operating correctly in the production system.
- The production system is free from security compromises and provides information on the nature and extent of compromises as feasible, should they occur.
- The management of change program is being rigorously followed with an audit trail of reviews and approvals for all changes.

The results from each periodic audit should be expressed in the form of performance against a set of predefined and appropriate metrics to display security performance and security trends. Security performance metrics should be sent to the appropriate stakeholders, along with a view of security performance trends.

Traditionally, the primary basis for audit in IT systems has been recordkeeping. Using appropriate tools within an ICS environment requires extensive knowledge from an IT professional familiar with critical production and safety implications for the facility. Many of the process control devices that are integrated into the ICS have been installed for many years and do not have the capability to provide the audit records described in this section. Therefore, the applicability of these more modern tools for auditing system and network activity is dependent upon the capabilities of the components in the ICS.

The critical tasks in managing a network in an ICS environment are ensuring reliability and availability to support safe and efficient operation. In regulated industries, regulatory compliance can add complexity to security and authentication management, registry and installation integrity management, and all functions that can augment an installation and operational qualification exercise.

Diligent use of auditing and log management tools can provide valuable assistance in maintaining and proving the integrity of the ICS from installation through the system life cycle.

The value of these tools in this environment can be calculated by the effort required to re qualify or otherwise retest the ICS where the integrity due to attack, accident, or error is in question. The system should provide reliable, synchronized time stamps in support of the audit tools.

Monitoring of sensors, logs, IDS, antivirus, patch management, policy management software, and other security mechanisms should be done on a real-time basis where feasible. A first-line monitoring service would receive alarms, do rapid initial problem determination and take action to alert appropriate facility personnel to intervene.

System auditing utilities should be incorporated into new and existing ICS projects. These tools can provide tangible records of evidence and system integrity. Additionally, active log management utilities may actually flag an attack or event in progress and provide location and tracing information to help respond to the incident [34].

There should be a method for tracing all console activities to a user, either manually (e.g., control room sign in) or automatic (e.g., login at the application and/or OS layer). Policies and procedures for what is logged, how the logs are stored (or printed), how they are protected, who has access to the logs and how/when are they reviewed should be developed. These policies and procedures will vary with the ICS application and platform. Legacy systems typically employ printer loggers, which are reviewed by administrative, operational, and security staff. Logs maintained by the ICS application may be stored at various locations and may or may not be encrypted.

6.3.4 System and Communications Protection

The security controls that fall within the NIST SP 800-53 System and Communications Protection (SC) family provide policy and procedures for protecting systems and data communications components.

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

- NIST SP 800-28 provides guidance on active content and mobile code [71].
- NIST SP 800-52 provides guidance on Transport Layer Security (TLS) Implementations [72]
- NIST SP 800-56 provides guidance on cryptographic key establishment [73].
- NIST SP 800-57 provides guidance on cryptographic key management [74].
- NIST SP 800-58 provides guidance on security considerations for VoIP technologies [75].
- NIST SP 800-63 provides guidance on remote electronic authentication [54].
- NIST SP 800-77 provides guidance on IPsec VPNs [76].

6.3.4.1 Encryption

Encryption is the cryptographic transformation of data (called plaintext) into a form (called ciphertext) that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called decryption, which is a transformation that restores encrypted data to its original state [77].

ICS Specific Recommendations and Guidance

The use of encryption within an ICS environment could introduce communications latency due to the additional time and computing resources required to encrypt, decrypt, and authenticate each message. For ICS, any latency induced from the use of encryption, or any other security technique, must not degrade the operational performance of the end device. Encryption at OSI Layer 2 should be considered, rather than at Layer 3 to reduce encryption latency.

In addition, encrypted messages are often larger than unencrypted messages due to one or more of the following:

- Additional checksums to reduce errors
- Protocols to control the cryptography
- Padding (for block ciphers)
- Authentication procedures
- Other required cryptographic processes.

Cryptography also introduces key management issues. Sound security policies require periodic key changes. This process becomes more difficult as the geographic size of the ICS increases, with extensive SCADA systems being the most severe example. Because site visits to change keys can be costly and slow, it is useful to be able to change keys remotely.

Before deploying encryption, first determine if encryption is the appropriate solution for the specific ICS application, as authentication and integrity are generally the key security issues for ICS applications. If cryptography is selected, the most effective safeguard is to use a complete cryptographic system approved by the NIST/ Communications Security Establishment (CSE) Cryptographic Module Validation Program (CMVP)20.

Within this program standards are maintained to ensure that cryptographic systems were studied carefully for weaknesses by a wide range of experts, rather than being developed by a few engineers in a single organization.

At a minimum, certification makes it probable that:

- Some method (such as counter mode) will be used to ensure that the same message does not generate the same value each time
- ICS messages are protected against replay and forging
- Key management is secure throughout the life cycle of the key
- The system is using an effective random number generator
- The entire system has been implemented securely.

Even then, the technology is only effective if it is an integral part of an effectively enforced information security policy. American Gas Association (AGA) report 12-1 [5] contains an example of such a security policy. While it is directed toward a gas SCADA system, many of its policy recommendations could apply to any ICS.

For an ICS, encryption can be deployed as part of a comprehensive, enforced security policy. Organizations should select cryptographic protection matched to the value of the information being protected and ICS operating constraints. Specifically, a cryptographic key should be long enough so that guessing it or determining it through analysis takes more effort, time, and cost than the value of the protected asset.

The encryption hardware should be protected from physical tampering and uncontrolled electronic connections. Assuming cryptography is the appropriate solution, organizations should select cryptographic protection with remote key management if the units being protected are so numerous or geographically dispersed that changing keys is difficult or expensive. [34]

6.3.4.2 Virtual Private Network (VPN)

One method of encrypting communication data is through a VPN, which is a private network that operates as an overlay on a public infrastructure, so that the private network can function across a public network. The most common types of VPN technologies implemented today are:

Internet Protocol Security (IPsec). IPsec is a set of standards defined by IETF to govern the secure communications of data across public networks at the IP layer. IPsec is included in many current operating systems. The intent of the standards is to guarantee interoperability across vendor platforms; however, the reality is that the determination of interoperability of multi-vendor implementations depends on specific implementation testing conducted by the end-user organization. IPsec supports two encryption modes: transport and tunnel. Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. The more secure tunnel mode adds a new header to each packet and encrypts both the original header and the payload. On the receiving side, an IPsec-compliant device decrypts each packet. The protocol has been continually enhanced to address specific requirements, such as extensions to the protocol to address individual user authentication and NAT device transversal. These extensions are typically vendor-specific and can lead to interoperability issues primarily in host-to-security gateway environments. NIST SP 800-77 provides guidance on IPsec VPNs.

Secure Sockets Layer (SSL). SSL provides a secure channel between two machines that encrypts the contents of each packet. The IETF made slight modifications to the SSL version 3 protocol and created a new protocol called Transport Layer Security (TLS). The terms “SSL” and “TLS” are often used interchangeably, and this document generically uses the SSL terminology. SSL is most often recognized for securing HTTP traffic; this protocol implementation is known as HTTP Secure (HTTPS). However, SSL is not limited to HTTP traffic; it can be used to secure many different application layer programs. SSL-based VPN products have gained acceptance because of the market for “clientless” VPN products. These products use standard Web browsers as clients, which have built-in SSL support. The “clientless” term means that there is no need to install or configure third-party VPN “client” software on users’ systems. NIST SP 800-52 provides guidance on SSL configuration.

Secure Shell (SSH). SSH is a command interface and protocol for securely gaining access to a remote computer. It is widely used by network administrators to remotely control Web servers and other types of servers. The latest version, SSH2, is a proposed set of standards from the IETF. Typically, SSH is deployed as a secure alternative to a telnet application. SSH is included in most UNIX distributions, and is typically added to other platforms through a third-party package.

ICS Specific Recommendations and Guidance

VPNs are most often used in the ICS environment to provide secure access from an untrusted network to the ICS control network. Untrusted networks can range from the Internet to the corporate LAN. Properly configured, VPNs can greatly restrict access to and from control system host computers and controllers, thereby improving security. They can also potentially improve control network responsiveness by removing unauthorized non-essential traffic from the intermediary network. VPN devices used to protect control systems should be thoroughly tested to verify that the VPN technology is compatible with the application and that the VPN devices do not unacceptably affect network traffic characteristics of the implementation [34].

Topic 6 – ICS Security Controls Section References

[41] Wack, John, et al., NIST SP 800-42, *Guideline on Network Security Testing*, 2003, http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf.

[42] Roback, Edward, NIST SP 800-23, *Guidelines to Federal Organizations on Security Assurance and Acquisition/ Use of Tested/Evaluated Products*, 2000, http://csrc.nist.gov/publications/nistpubs/800-23/sp800-23.pdf.

[43] Stoneburner, Gary, et al., NIST SP 800-27, *Engineering Principles for Information Security (A Baseline for Achieving Security), Revision A*, 2004, http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.

[44] Grance, Tim, et al., NIST SP 800-35, *Guide to Information Technology Security Services*, 2003, http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf.

[45] Grance, Tim, et al., NIST SP 800-36, *Guide to Selecting Information Technology Security Products*, 2003, http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf.

[46] Grance, Tim, et al., NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle*, Revision 1, 2004, http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf.

[47] Hash, Joan, et al., NIST SP 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*, 2005, http://csrc.nist.gov/publications/nistpubs/800-65/SP-800-65-Final.pdf.

[48] System Protection Profile – Industrial Control Systems (SPP-ICS), NIST Internal Report, http://www.isd.mel.nist.gov/projects/processcontrol/SPP-ICSv1.0.pdf.

[49] SCADA and Control Systems Procurement Project, http://www.cscic.state.ny.us/msisac/scada/.

[50] Dray, James, et al., NIST SP 800-73, *Interfaces for Personal Identity Verification*, 2005, http://csrc.nist.gov/publications/nistpubs/800-73/SP800-73-Final.pdf.

[51] Wilson, Charles, et al., NIST SP 800-76, *Biometric Data Specification for Personal Identity Verification*, 2006, http://csrc.nist.gov/publications/nistpubs/800-76/sp800-76.pdf.

[52] Kuhn, D. Richard, et al., NIST SP 800-46, *Security for Telecommuting and Broadband Communications*, 2002, http://csrc.nist.gov/publications/nistpubs/800-46/sp800-46.pdf.

[53] Swanson, Marianne, et al., NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, 2002, http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf.

[54] Burr, William, et al., NIST SP 800-63, *Electronic Authentication Guideline*, 2004, http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf.

[55] Bace, Rebecca, and Mell, Peter, NIST SP 800-31, *Intrusion Detection Systems*, 2001, http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf.

[56] Kent, Karen, and Mell, Peter, NIST SP 800-94, *Guide to Intrusion Detection and Prevention (IDP) Systems*, 2006, http://csrc.nist.gov/publications/drafts/Draft-SP800-94.pdf

[57] Falco, Joe, et al., *Using Anti-virus Software on Industrial Control Systems: Integration Guidance and a Test Methodology for Assessing Performance Impacts*, 2006, Draft Document, http://www.isd.mel.nist.gov/projects/processcontrol/AV_Guide_PCSF_Draft_Release_20060530.pdf

[58] Peterson, Dale, *Intrusion Detection and Cyber Security Monitoring of SCADA and DCS Networks*, ISA, 2004, http://www.digitalbond.com/SCADA_security/ISA%20Automation%20West.pdf.

[59] *Symantec Expands SCADA Protection for Electric Utilities*, http://www.symantec.com/about/news/release/article.jsp?prid=20050914_01

[60] Digital Bond, http://www.digitalbond.com/support-center/.

[61] Grance, Tim, et al., NIST SP 800-61, *Computer Security Incident Handling Guide*, 2004, http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf.
[62] Mell, Peter, et al., NIST SP 800-83, *Guide to Malware Incident Prevention and Handling*, 2005, http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf.
[63] Wilson, Mark, and Hash, Joan, NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, 2003, http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.
[64] Mix, S., *Supervisory Control and Data Acquisition (SCADA) Systems Security Guide*, EPRI, 2003.
[65] Karygiannis, Tom, and Owens, Les, NIST SP 800-48, *Wireless Network Security, 802.11, Bluetooth and Handheld Devices*, 2002, http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf.
[66] Frankel, Sheila, et al, NIST SP800-97 Draft, *Guide to IEEE 802.11i: Establishing Robust Security Networks*, 2006, http://csrc.nist.gov/publications/drafts/Draft-SP800-97.pdf
[67] Federal Information Processing Standards Publication: FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, NIST, 2006, http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf
[68] Dray, James, et al, NIST SP 800-96, *PIV Card to Reader Interoperability Guidelines*, 2006, http://csrc.nist.gov/publications/nistpubs/800-96/SP800-96-091106.pdf
[69] Polk, W., Timothy, et al, NIST SP800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, 2005, http://csrc.nist.gov/publications/nistpubs/800-78/sp800-78-final.pdf
[70] Souppaya, Murugiah, Kent, Karen, NIST SP800-92, Guide to Computer Security Log Management, 2006, http://csrc.nist.gov/publications/drafts/DRAFT-SP800-92.pdf
[71] Jansen, Wayne, NIST SP 800-28, *Guidelines on Active Content and Mobile Code*, 2001, http://csrc.nist.gov/publications/nistpubs/800-28/sp800-28.pdf.
[72] Chernick, Michael, et al, NIST SP 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations, 2005, http://csrc.nist.gov/publications/nistpubs/800-52/SP800-52.pdf
[73] Barker, Elaine, et al., NIST SP 800-56, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, 2005, http://csrc.nist.gov/publications/drafts/SP800-56_7-5-05.pdf.
[74] Baker, Elaine, et al., NIST SP 800-57, Recommendation for Key Management, 2005, Part 1, General: http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part1.pdf, Part 2, Best Practices: http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part2.pdf.
[75] Kuhn, D. Richard, et al., NIST SP 800-58, *Security Recommendations for Voice Over IP Systems*, 2005, http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf.
[76] Frankel, Sheila, et al, NIST SP 800-77, *Guide to IPsec* VPNs, 2005, http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf.
[77] Internet Security Glossary: RFC 2828, http://rfc.net/rfc2828.html.
[78] Franz, Matthew, and Pothamsetty, Venkat, *ModbusFW Deep Packet Inspection for Industrial Ethernet*, Critical Infrastructure Assurance Group, Cisco Systems, 2004, http://www.scadasec.net/oldio/papers/franz-niscc-modbusfw-may04.pdf.
[79] Duggan, David, *Penetration Testing of Industrial Control Systems*, Report SAND2005-2846P, Sandia National Laboratories, 2005, http://www.sandia.gov/scada/documents/sand_2005_2846p.pdf.
[80] Kissel, Richard, et al., NIST SP 800-88, *Guidelines for Media Sanitization,* 2006,

Topic 6 – ICS Security Controls Section Post Quiz

True or False

1. Security controls are the management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an informational system to protect the confidentiality, integrity, and availability of the system and its information.
True or False

2. A single security product or technology cant adequately protect an ICS.
True or False

3. Securing an ICS is based on a combination of effective operator input.
True or False

4. An effective cyber security strategy for an ICS should apply defense-in-depth, a technique of layering security mechanisms so that the impact of a failure in any one mechanism is minimized. True or False

5. Certification, Accreditation, and Security Assessments is the allocation of resources for information system security to be maintained throughout the systems life cycle and the development of acquisition policies based on risk assessment results including requirements, design criteria, test procedures, and associated documentation.
True or False

6. System and Services Acquisition is the assurance that the specified controls are implemented correctly, operating as intended, and producing the desired outcome.
True or False

7. Planning is the process of identifying risks to operations, assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. True or False

8. Risk Assessment is the development and maintenance of a plan to address information system security by performing assessments, specifying and implementing security controls, assigning security levels, and responding to incidents.
True or False

9. Achieving an acceptable level of risk is a process of reducing the probability of an incident that is accomplished by mitigating or eliminating vulnerabilities that can be exploited as well as consequences resulting from an incident.
True or False

10. Prioritization of vulnerabilities must be based on cost and benefit with an objective to provide a business case for implementing at least a minimum set of control system security requirements to reduce risk to an acceptable level. True or False

11. A mistake often made during a risk assessment is to select static vulnerabilities is taking into account the level of risk associated with them. True or False

12. Vulnerabilities should be assessed and rated for risk after trying to select and implement security controls on them. True or False

13. A security plan is a guideline that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements. True or False

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

15. The security requirements of an organization outsourcing the management and control of all or some of its information systems, networks, and desktop environments should be addressed in a contract agreed between the parties. True or False

Glossary

A/D Converter (analog to digital): A device that converts continuous analog signal into discrete digital signals.

Actuator: A fluid powered or electric powered device that supplies force and motion.

Algorithm: A set of well-defined rules or processes for solving a mathematical problem in a finite number of steps.

Analog: A variable that may be continuously observed and controlled.

BPS bits per second: Bit transmission rate in digital communication.

Building Management System: This is a system designed to control doors, elevators, access control, CCTV cameras and display their footage. They often contain some energy management elements and sometimes HVAC as well. Compromising one of these can lead to physical site compromise or CCTV footage of personnel and their daily tasks.

Carrier Wave: A sinusoidal waveform that can be modulated with an input signal to carry information.

D/A Converter (digital to analog): A device for converting a discrete digital signal into an analog signal.

Demodulation: To extract the original information from a modulated carrier signal.

Discrete: Consisting of distinct parts.

DMS: Distribution Management System. A SCADA server tailored for the energy distribution companies.

Embedded Web Server: These are micro webservers designed for embedded systems. They are commonly found in industrial system devices, but also in many other embedded system devices. Disambiguating those designed for industrial systems from others is sometimes necessary.

EMS: Energy Management System. Essentially a SCADA server tailored for the energy industry. In some cases, this will refer to a large electrical network, and in other products, this refers to the energy used within a building. From a technical point of view, they are similar, but the criticality of the former is likely to be national and the criticality of the latter much reduced to that of a few businesses.

Full Duplex: A method of operation for a communication circuit where each end can simultaneously transmit and receive.

Half Duplex: A method of operation for communication circuit where each end can either transmit or receive, but not simultaneously.

Historian: These computers store values for various processes or states of interest to the industrial system. Sometimes they are regulatory records, and provide data reporting functionality designed to translate raw engineering values into CEO level reports. They are often the point of connection between the corporate network and the control network.

HMI: Human Machine Interface sometimes called the (Man Machine Interface) MMI or (Human Computer Interface) HCI. These are nodes at which control engineers monitor their plants, factories, pipelines, and field devices. Often found in control rooms, but sometimes dispersed across the plant floor. These are often running a well-known operating system and any internet reachability is of particular concern as these nodes are in control of field or plant devices. Anecdotally, changing a display on an HMI can cause an operator to perform a detrimental safety critical action under false pretences, in a similar manner to Phishing attacks on banking customers today.

Home Area/Automation Network: This is a small energy management system for the home, but also refers to the appliances in the home which will communicate with it to determine the best time of day to function while saving energy or money. The smart meter may be part of this system directly or indirectly.

I/O (Input/Output): The device used to communicate between the computer and the operator.

ICS: A system that performs the functions of target acquisition, tracking, data computation, and engagement control, primarily using electronic means and assisted by electromechanical devices.

IED: Intelligent Electronic Device. This performs similar functions to a PLC, but is primarily deployed in the electrical sector, for example in substations. Since these devices sometimes have to function in the presence of high voltages, they can be constructed with substantial protections for hostile environments. However, from an outsider's perspective they still gather data, provide protective logic, and execute simple controls as does a PLC or RTU.

LAN: Local area network.

Meter: A meter is a device capable of providing telemetry readings, and is functionally the same as your electrical meter. However, in process control they serve a different purpose such as monitoring the energy going through each substation, or water purified per day to measure business efficiency. Some meters are process critical, in that they monitor the levels of a chemical into a water supply, or amount of water into a reactor cooling tower. Others are much smaller and cheaper, and only serve to show the electricity you consume in a home.

Modulation: To vary or change a carrier wave with digital data.

MTU (Master Terminal Unit): In SCADA, the device that interfaces with the operator providing long-term storage of data, and handles communication.

PAC: Programmable Automation Controller. These provide very similar functions to PLCs, but are programmed differently, and use an open, modular, architecture. They typically differ in how they do things from PLCs, but still serve the same purpose of acquiring data and performing process control.

PLC: Programmable Logic Controller. These are similar to RTUs, but are more often deployed without their own power supply and using wired communications. They are more often found on a plant or factory, where controllers are close to the centre of control.

Protocol Bridge: These are points where one protocol is translated to another. Mainly in our study, these are points where TCP/IP traffic is converted to some (often proprietary) control protocol such as Modbus, LonWorks, BACNet, etc. These other protocols are often industry specific and there are too many serving different purposes to list them all here. We are interested in these bridges because they are specifically places where an automation or control network connects to an IP network. Thus, it is a great place to look for the internet connectivity of an industrial system.

Protocol: A set of rules and formats that determines the communication behavior of a system.

Real Time: In SCADA, pertaining to performing computations during the actual time that the related process takes place.

Register: The specific location of data in a memory bank.

RTU (Remote Terminal Unit): In SCADA, the device that is located away from the central control area. Remote Terminal Unit or sometimes Remote Telemetry Unit. This is a microprocessor used to transmit telemetry back from the field and to control devices in the field. They are often widely geographically dispersed, and use diverse wireless communications accordingly. They can run simple safety logic programs for redundancy and to reduce control delays.

SCADA Server: Supervisory Control and Data Acquisition Server. This system typically interacts with multiple HMIs and control engineers. They are often replicated for redundancy and availability reasons.

SCADA: Supervisory Control and Data Acquisition

Sensor: An element that receives data about the process and converts it to a form that is usable by the control system.

Simplex: A method of data transmission whereby data can be transferred in one direction only.

Telemetry: This is the sensor data, process data, and other engineering values of interest to control engineers. It may also refer to the server used to collect such data and there is some crossover in these systems with an Historian.

Telemetry: Transmitting the readings of a distant measuring instrument.

Totalizer: A device that receives signals and applies an algorithm to determine the amount of product that has been measured.

UPS: Uninterruptible Power Supply an electric battery based system for providing continues power to critical equipment during a power loss.

1xRTT - (Single Carrier (1x) Radio Transmission Technology): A wireless communications *protocol* used for connections to *networks* by devices such as laptop computers. 1xRTT has the capability of providing data transfer speeds of up to 144 thousand *bps*. 1xRTT is a built on top of another widely used protocol, *CDMA* and is also called CMDA2000.

ADN -- (Advanced Digital Network): Usually refers to a 56K*bps leased-line*.

ADSL - (Asymmetric Digital Subscriber Line): A *DSL* line where the upload speed is different from the download speed. Usually the download speed is much greater.

Ajax - (Asynchronous JavaScript and XML):A way of including content in a *web page* in which *javascript* code in the web page fetches some data from a server and displays it without re-fetching the entire surrounding page at the same time (hence the 'Asynchronous').

Apache: The most common web server (or *HTTP* server) software on the Internet. Apache is an open-source application originally created from a series of changes ("patches") made to a web server written at the National Center for Supercomputing Applications, the same place the *Mosaic* web browser was created. Apache is designed as a set of modules, enabling administrators to choose which features they wish to use and making it easy to add features to meet specific needs including handling protocols other than the web-standard *HTTP*.

Applet: A small *Java* program that can be embedded in an *HTML* page. Applets differ from full-fledged Java applications in that they are not allowed to access certain resources on the local computer, such as files and serial devices (modems, printers, etc.), and are prohibited from communicating with most other computers across a network. The common rule is that an applet can only make an Internet connection to the computer from which the applet was sent.

Application Server: *Server* software that manages one or more other pieces of software in a way that makes the managed software available over a network, usually to a *Web* server. By having a piece of software manage other software packages it is possible to use resources like memory and database access more efficiently than if each of the managed packages responded directly to requests.

Archie: A tool (software) for finding files stored on *anonymous FTP* sites. You need to know the exact file name or a substring of it. By 1999, *Archie* had been almost completely replaced by web-based search engines. Back when *FTP* was the main way people moved files over the *Internet* Archie was quite popular.

ARPANet - (Advanced Research Projects Agency Network): The precursor to the *Internet*. Developed in the late 60's and early 70's by the US Department of Defense as an experiment in wide-area-networking to connect together computers that were each running different system so that people at one location could use computing resources from another location.

ASCII - (American Standard Code for Information Interchange): This is the de-facto world-wide standard for the code numbers used by computers to represent all the upper and lower-case Latin letters, numbers, punctuation, etc. There are 128 standard ASCII codes each of which can be represented by a 7 digit binary number: 0000000 through 1111111.

ASP - (Application Service Provider): An organization (usually a business) that runs one or more applications on their own servers and provides (usually for a fee) access to others.

Backbone: A high-speed line or series of connections that forms a major pathway within a network. The term is relative as a backbone in a small *network* will likely be much smaller than many non-backbone lines in a large network.

Bandwidth: In common, usage the term "bandwidth" is used to describe how much stuff you can send through a network connection, in other words "bandwidth" is used as a synonym for the speed or *throughput* of the connection.

Baud: In common, usage the "baud" of a *modem* is how many *bits* it can send or receive per second. Technically, baud is the number of times per second that the carrier signal shifts value - for example, a 1200 bit-per-second modem actually runs at 300 baud, but it moves 4 bits per baud (4 x 300= 1200 bits per second).

BBS - (Bulletin Board System): A computerized meeting and announcement system that allows people to carry on discussions, upload and download files, and make announcements without the people being connected to the computer at the same time..

Binary: Information consisting entirely of ones and zeros. Also, commonly used to refer to files that are not simply text files, e.g. images.

Binhex - (BINary HEXadecimal): A method for converting non-text files (non-ASCII) into *ASCII*. This is needed because Internet e-mail can only handle ASCII.

bps - (Bits-Per-Second): A measurement of how fast data is moved from one place to another. A 56K *modem* can move about 57,000 bits per second.

Broadband: Generally refers to connections to the Internet with much greater *bandwidth* than you can get with a *modem*. There is no specific definition of the speed of a "broadband" connection but in general any Internet connection using *DSL* or a via Cable-TV may be considered a broadband connection.

Browser: A *Client* program (software) that is used to look at various kinds of Internet resources.

BTW - (By The Way): A shorthand appended to a comment written in an online forum.

Byte: A set of Bits that represent a single character. Usually there are 8 Bits in a Byte, sometimes more, depending on how the measurement is being made.

CDMA - (Code Division Multiple Access): A *protocol* for wireless data and voice communication, CMDA is widely used in cellphone networks, but also in many other data communications systems. CDMA uses a technique called "Spread Spectrum" whereby the data being transmitted is spread across multiple radio frequencies, making more efficient use of available radio spectrum. There are a number of additional protocols built on top of CDMA, such as *1xRTT* (also called CMDA2000).

Certificate Authority: An issuer of *Security Certificates* used in *SSL* connections.

CGI - (Common Gateway Interface): A set of rules that describe how a *Web Server* communicates with another piece of software on the same machine, and how the other piece of software (the “CGI program”) talks to the web server. Any piece of software can be a CGI program if it handles input and output according to the CGI standard.

Cgi-bin: The most common name of a directory on a web server in which *CGI* programs are stored.

Client: A software program that is used to contact and obtain data from a *Server* software program on another computer, often across a great distance. Each *Client* program is designed to work with one or more specific kinds of *Server* programs, and each *Server* requires a specific kind of *Client*. A Web *Browser* is a specific kind of *Client.*

Co-location: Most often used to refer to having a *server* that belongs to one person or group physically located on an *Internet*-connected *network* that belongs to another person or group. Usually this is done because the server owner wants their machine to be on a high-speed Internet connection and/or they do not want the security risks of having the server on their own network.

Cookie: The most common meaning of "Cookie" on the Internet refers to a piece of information sent by a Web *Server* to a Web *Browser* that the Browser software is expected to save and to send back to the Server whenever the browser makes additional requests from the Server. Depending on the type of Cookie used, and the Browsers' settings, the Browser may accept or not accept the Cookie, and may save the Cookie for either a short time or a long time. Cookies might contain information such as login or registration information, online"

CSS - (Cascading Style Sheet): A standard for specifying the appearance of text and other elements. CSS was developed for use with *HTML* in *Web pages* but is also used in other situations, notably in applications built using *XPFE*. CSS is typically used to provide a single "library" of styles that are used over and over throughout a large number of related documents, as in a web site. A CSS file might specify that all numbered lists are to appear in *italics*. By changing that single specification the look of a large number of documents can be easily changed.

DHCP - (Dynamic Host Configuration Protocol): DHCP is a *protocol* by which a machine can obtain an *IP number* (and other network configuration information) from a *server* on the local *network*.

DHTML - (Dynamic HyperText Markup Language): DHTML refers to *web pages* that use a combination of *HTML*, *JavaScript*, and *CSS* to create features such as letting the user drag items around on the web page, some simple kinds of animation, and many more.

Digerati: The digital version of literati, it is a reference to a vague cloud of people seen to be knowledgeable, hip, or otherwise in-the-know in regards to the digital revolution.

DNS - (Domain Name System):The Domain Name System is the system that translates Internet *domain names* into *IP numbers*. A "DNS Server" is a *server* that performs this kind of translation.

Ethernet: A very common method of networking computers in a *LAN*. There is more than one type of Ethernet. By 2001, the standard type was "100-BaseT" which can handle up to about 100,000,000 bits-per-second and can be used with almost any kind of computer.

Extranet: An *intranet* that is accessible to computers that are not physically part of a company's' own private *network*, but that is not accessible to the general public, for example to allow vendors and business partners to access a company web site. Often an intranet will make use of a Virtual Private Network. (*VPN*.)

FDDI - (Fiber Distributed Data Interface):A standard for transmitting data on optical fiber cables at a rate of around 100,000,000 bits-per-second (10 times as fast as 10-BaseT*Ethernet*, about twice as fast as *T-3*).

Finger: An Internet software tool for locating people on other Internet sites. Finger is also sometimes used to give access to non-personal information, but the most common use is to see if a person has an account at a particular Internet site. Many sites do not allow incoming Finger requests, but many do.

Fire Wall: A combination of hardware and software that separates a *Network* into two or more parts for security purposes.

FTP - (File Transfer Protocol): A very common method of moving files between two Internet sites. FTP is a way to *login* to another Internet site for the purposes of retrieving and/or sending files. There are many Internet sites that have established publicly accessible repositories of material that can be obtained using FTP, by logging in using the account name "anonymous", thus, these sites are called "anonymous ftp servers".

IMAP - (Internet Message Access Protocol): IMAP is gradually replacing *POP* as the main protocol used by email *clients* in communicating with email *servers*.

internet (Lower case i): Any time you connect 2 or more *networks* together, you have an internet - as in inter-national or inter-state.

Internet (Upper case I): The vast collection of inter-connected networks that are connected using the *TCP/IP* protocols and that evolved from the *ARPANET* of the late 60's and early 70's.

Intranet: A private *network* inside a company or organization that uses the same kinds of software that you would find on the public *Internet*, but that is only for internal use. Compare with *extranet*.

IP Number - (Internet Protocol Number): Sometimes called a dotted quad. A unique number consisting of 4 parts separated by dots, e.g. 165.114.243.2 Every machine that is on the Internet has a unique IP number - if a machine does not have an IP number, it is not really on the Internet. Many machines (especially servers) also have one or more Domain Names that are easier for people to remember.

IPv4 - (Internet Protocol, version 4): The most widely used version of the Internet Protocol (the "IP" part of *TCP/IP*.) IPv4 allows for a theoretical maximum of approximately four billion *IP Numbers* (technically 2^{32}), but the actual number is far less due to inefficiencies in the way blocks of numbers are handled by networks. The gradual adoption of *IPv6* will solve this problem.

IPv6 - (Internet Protocol, version 6): The successor to *IPv4*. Already deployed in some cases and gradually spreading, IPv6 provides a huge number of available *IP Numbers* - over a sextillion addresses (theoretically 2^{128}). IPv6 allows every device on the planet to have its own IP Number.

IRC - (Internet Relay Chat): Basically a huge multi-user live chat facility. There are a number of major IRC *servers* around the world which are linked to each other. Anyone can create a channel and anything that anyone types in a given channel is seen by all others in the channel. Private channels can (and are) created for multi-person conference calls.

ISDN - (Integrated Services Digital Network):Basically a way to move more data over existing regular phone lines. ISDN is available to much of the USA and in most markets it is priced very comparably to standard analog phone circuits. It can provide speeds of roughly 128,000 bits-per-second over regular phone lines. In practice, most people will be limited to 56,000or 64,000 bits-per-second.

ISP - (Internet Service Provider): An institution that provides access to the Internet in some form, usually for money.

IT - (Information Technology): A very general term referring to the entire field of Information Technology - anything from computer hardware to programming to network management. Most medium and large size companies have IT Departments.

JavaScript: JavaScript is a programming language that is mostly used in web pages, usually to add features that make the web page more interactive. When JavaScript is included in an *HTML* file it relies upon the browser to interpret the JavaScript. When JavaScript is combined with *Cascading Style Sheets* (CSS), and later versions of HTML (4.0 and later) the result is often called *DHTML*.

JDK - (Java Development Kit): A software development package from Sun Microsystems that implements the basic set of tools needed to write, test and debug *Java* applications and *applets*

LAN - (Local Area Network): A computer network limited to the immediate area, usually the same building or floor of a building.

Leased Line: Refers to line such as a telephone line or fiber-optic cable that is rented for exclusive 24-hour, 7-days-a-week use from your location to another location. The highest speed data connections require a leased line.

Linux: A widely used Open Source Unix-like operating system. Linux was first released by its inventor Linus Torvalds in 1991. There are versions of Linux for almost every available type of computer hardware from desktop machines to IBM mainframes.

Meta Tag: A specific kind of *HTML* tag that contains information not normally displayed to the user. Meta tags contain information about the page itself, hence the name ("meta" means "about this subject")

MIME - (Multipurpose Internet Mail Extensions): Originally, a standard for defining the types of files attached to standard Internet mail messages. The MIME standard has come to be used in many situations where one computer programs needs to communicate with another program about what kind of file is being sent.

Mirror: Generally speaking, "to mirror" is to maintain an exact copy of something. Probably the most common use of the term on the Internet refers to "mirror sites" which are *web* sites, or *FTP* sites that maintain copies of material originated at another location, usually in order to provide more widespread access to the resource. For example, one site might create a library of software, and 5 other sites might maintain mirrors of that library.

Modem - (MOdulator, DEModulator): A device that connects a computer to a phone line. A telephone for a computer. A modem allows a computer to talk to other computers through the phone system. Modems do for computers what a telephone does for humans. The maximum practical *bandwidth* using a modem over regular telephone lines is currently around 57,000 *bps*.

Mod_perl: An add-on for the *Apache* web server software, mod_perl makes it possible to use the Perl language to add new features for the Apache server, and to increase the speed of Perl applications by as much as 30 times.

Mosaic: The first *WWW browser* that was available for the Macintosh, Windows, and UNIX all with the same interface. Mosaic really started the popularity of the Web. The source-code to Mosaic was licensed by several companies and used to create many other web browsers.

Netizen: Derived from the term citizen, referring to a citizen of the *Internet*, or someone who uses networked resources. The term connotes civic responsibility and participation.

Netscape: A *WWW Browser* and the name of a company. The Netscape (tm) browser was originally based on the *Mosaic* program developed at the National Center for Supercomputing Applications (NCSA).

Network: Any time you connect 2 or more computers together so that they can share resources, you have a computer network. Connect 2 or more networks together and you have an *internet*.

Newsgroup: The name for discussion groups on *USENET*.

NIC - (Network Information Center): Generally, any office that handles information for a network. The most famous of these on the Internet was the InterNIC, which was where most new domain names were registered until that process was decentralized to a number of private companies. Also means "Network Interface card", which is the card in a computer that you plug a network cable into.

NNTP -- (Network News Transport Protocol): The protocol used by *client* and *server* software to carry *USENET* postings back and forth over a *TCP/IP network*. If you are using any of the more common software such as *Netscape*, Nuntius, Internet Explorer, etc. to participate in *newsgroups* then you are benefiting from an NNTP connection.

Node: Any single computer connected to a *network*.

Perl - (Practical Extraction and Report Language): Perl is a programming language that is widely used for both very simple, small tasks and for very large complex applications.

Permalink: A "permanent link" to a particular posting in a *blog*. A permalink is a *URI* that points to a specific blog posting, rather than to the page in which the posting original occurred (which may no longer contain the posting.)

PHP - (PHP: Hypertext Preprocessor): PHP is a programming language used almost exclusively for creating software that is part of a *web site*. The PHP language is designed to be intermingled with the *HTML* that is used to create *web pages*. Unlike HTML, the PHP code is read and processed by the web *server* software (HTML is read and processed by the web *browser* software.)

Ping: To check if a server is running. From the sound that a sonar systems makes in movies, you know, when they are searching for a submarine.

Plug-in: A (usually small) piece of software that adds features to a larger piece of software. Common examples are plug-ins for the Netscape® *browser* and web *server*. Adobe Photoshop® also uses plug-ins.

PNG - (Portable Network Graphics): PNG is a graphics format specifically designed for use on the World Wide Web. PNG enable compression of images without any loss of quality, including high-resolution images. Another important feature of PNG is that anyone may create software that works with PNG images without paying any fees - the PNG standard is free of any licensing costs.

POP - (Point of Presence, also Post Office Protocol):Two commonly used meanings: Point of Presence and Post Office Protocol. A Point of Presence usually means a city or location where a network can be connected to, often with dial up phone lines. Therefore, if an Internet company says they will soon have a POP in Belgrade, it means that they will soon have a local phone number in Belgrade and/or a place where leased lines can connect to their network. A second meaning, Post Office Protocol refers to a way that e-mail *client* software such as Eudora gets mail from a mail *server*. When you obtain an account from an Internet Service Provider (*ISP*) you almost always get a POP account with it, and it is this POP account that you tell your e-mail software to use to get your mail. Another protocol called IMAP is replacing POP for email.

Port: 3 meanings. First and most generally, a place where information goes into or out of a computer, or both. E.g. the serial port on a personal computer is where a *modem* would be connected. On the Internet port often refers to a number that is part of a URL, appearing after a colon (:) right after the domain name. Every service on an Internet server listens on a particular port number on that server. Most services have standard port numbers, e.g. Web servers normally listen on port 80.

Portal: Usually used as a marketing term to described a Web site that is or is intended to be the first place people see when using the Web. Typically, a "Portal site" has a catalog of web sites, a search engine, or both. A Portal site may also offer email and other service to entice people to use that site as their main "point of entry" (hence "portal") to the Web.

Posting: A single message entered into a network communications system.

PPP - (Point to Point Protocol): The most common protocol used to connect home computers to the Internet over regular phone lines. Most well known as a protocol that allows a computer to use a regular telephone line

Protocol: On the Internet "protocol" usually refers to a set of rules that define an exact format for communication between systems. For example, the *HTTP* protocol defines the format for communication between web browsers and web servers, the *IMAP* protocol defines the format for communication between IMAP email servers and clients, and the *SSL* protocol defines a format for encrypted communications over the Internet.

Proxy Server: A Proxy Server sits in between a *Client* and the "real" *Server* that a Client is trying to use. Client's are sometimes configured to use a Proxy Server, usually an *HTTP* server. The clients makes all of it's requests from the Proxy Server, which then makes requests from the "real" server and passes the result back to the Client. Sometimes the Proxy server will store the results and give a stored result instead of making a new one (to reduce use of a *Network*). Proxy servers are commonly established on *Local Area Networks*

PSTN - (Public Switched Telephone Network): The regular old-fashioned telephone system.

RDF - (Resource Definition Framework): A set of rules (a sort of language) for creating descriptions of information, especially information available on the *World Wide Web*. RDF could be used to describe a collection of books, or artists, or a collection of *web pages* as in the *RSS* data format which uses RDF to create machine-readable summaries of web sites.

REST - (REpresentational State Transfer): A loosely defined specification for *HTTP*-based services where all of the information required to process a request is present in the initial request and where each request receives only a single response, and where the response is in a machine-readable form.

RFC - (Request For Comments): The name of the result and the process for creating a standard on the *Internet*. New standards are proposed and published on the Internet, as a Request For Comments.

Router: A special-purpose computer (or software package) that handles the connection between 2 or more Packet-Switched *networks*. Routers spend all their time looking at the source and destination addresses of the *packets* passing through them and deciding which route to send them on.

RSS - (Rich Site Summary or RDF Site Summary or Real Simple Syndication): A commonly used protocol for syndication and sharing of content, originally developed to facilitate the syndication of news articles, now widely used to share the contents of *blogs*. *Mashups* are often made using RSS feeds.

RTSP - (Real Time Streaming Protocol): RTSP is an official Internet standard (*RFC* 2326) for delivering and receiving streams of data such as audio and video. The standard allows for both real-time ("live") streams of data and streams from stored data.

SDSL - (Symmetric Digital Subscriber Line): A version of *DSL* where the upload speeds and download speeds are the same.

Security Certificate: A chunk of information (often stored as a text file) that is used by the *SSL* protocol to establish a secure connection.

SEO - (Search Engine Optimization):The practice of designing web pages so that they rank as high as possible in search results from *search engines*.

Server: A computer, or a software package, that provides a specific kind of service to *client* software running on other computers. A single server machine can (and often does) have several different server software packages running on it, thus providing many different servers to *clients* on the *network*. Sometimes server software is designed so that additional capabilities can be added to the main program by adding small programs known as *servlets*.

Servlet: A small computer program designed to be add capabilities to a larger piece of *server* software. Common examples are "Java servlets", which are small programs written in the *Java* language and which are added to a *web* server. Typically a web server that uses Java servlets will have many of them, each one designed to handle a very specific situation, for example one servlet will handle adding items to a "shopping cart", while a different servlet will handle deleting items from the "shopping cart."

SGML - (Standard Generalized Markup Language): Developed in 1986 SGML provides a rich set of rules for defining new data formats. A well-known example of using SGML is *XML*, which is a subset of SGML: The definition of XML is all of SGML minus a couple of dozen items. SGML is an International Standards Organization (ISO) standard: ISO 8879:1986.

SLIP - (Serial Line Internet Protocol): A standard that was popular in the early 1990's for using a regular telephone line (a serial line) and a *modem* to connect a computer as a real *Internet* site. SLIP has largely been replaced by *PPP*.

SMDS - (Switched Multimegabit Data Service): A standard for very high-speed data transfer.

SMTP - (Simple Mail Transfer Protocol): The main protocol used to send electronic mail from *server* to server on the Internet. SMTP is defined in *RFC* 821 and modified by many later RFC's.

SNMP - (Simple Network Management Protocol): A set of standards for communication with devices connected to a TCP/IP *network*. Examples of these devices include *routers*, hubs, and switches.

SOAP - (Simple Object Access Protocol): A *protocol* for *client-server* communication that sends and receives information "on top of" *HTTP*. The data sent and received is in a particular *XML* format specifically designed for use with SOAP. SOAP is similar to the *XMLRPC* protocol except that SOAP provides for more sophisticated handling of complex data being sent between a client and a server. SOAP actually grew from the work that created XMLRPC.

Spam (or Spamming): An inappropriate attempt to use a *mailing list*, or *USENET* or other networked communications facility as if it was a broadcast medium (which it is not) by sending the same message to a large number of people who didn’t ask for it.

SQL - (Structured Query Language):A specialized language for sending queries to databases. Most industrial-strength and many smaller database applications can be addressed using SQL. Each specific application will have its own slightly different version of SQL implementing features unique to that application, but all SQL-capable databases support a common subset of SQL.

SSL - (Secure Socket Layer):A protocol designed by Netscape Communications to enable encrypted, authenticated communications across the Internet.

Sysop-- (System Operator): Anyone responsible for the physical operations of a computer system or network resource. For example, a System Administrator decides how often backups and maintenance should be performed and the System Operator performs those tasks.

T-1: A *leased-line* connection capable of carrying data at 1,544,000 *bits*-per-second. At maximum theoretical capacity, a T-1 line could move a *megabyte* in less than 10 seconds. That is still not fast enough for full-screen, full-motion video, for which you need at least 10,000,000 bits-per-second. T-1 lines are commonly used to connect large *LAN*s to the *Internet*.

T-3: A *leased-line* connection capable of carrying data at 44,736,000 bits-per-second. This is more than enough to do full-screen, full-motion video.

Tag: The term "tag" can be used as a noun or verb. As a noun, a tag is a basic element of the languages used to create web pages (*HTML*) and similar languages such as *XML*. Another, more recent meaning of tag is related to reader-created tags where blogs and other content (such as photos, music, etc.) may be "tagged" which means to assign a keyword, such as "politics" or "gardening", this enables searches for "all the blog postings in the past week that are tagged 'prenatal care'"

TCP/IP - (Transmission Control Protocol/Internet Protocol):This is the suite of protocols that defines the *Internet*. Originally designed for the *UNIX* operating system, TCP/IP software is now included with every major kind of computer operating system. To be truly on the *Internet*, your computer must have TCP/IP software.

Telnet: The command and program used to *login* from one *Internet* site to another. The telnet command/program gets you to the login: prompt of another *host*.

Terabyte: 1000 *gigabytes*.

Terminal: A device that allows you to send commands to a computer somewhere else. At a minimum, this usually means a keyboard and a display screen and some simple circuitry. Usually you will use terminal software in a personal computer - the software pretends to be (emulates) a physical terminal and allows you to type commands to a computer somewhere else.

Terminal Server: A special purpose computer that has places to plug in many *modems* on one side, and a connection to a *LAN* or *host* machine on the other side. Thus, the terminal server does the work of answering the calls and passes the connections on to the appropriate *node*. Most terminal servers can provide *PPP* or *SLIP* services if connected to the *Internet*.

Throughput: How much stuff you can send through a connection. Throughput is what people usually mean when they use the term "Bandwidth" and it is usually measured in bits-per-second (*bps*.) A full page of English text is about 16,000 bits. A common configuration of *DSL* allows downloads at speeds of up to 1.544 megabits (not megabytes) per second, and uploads at speeds of 128 kilobits per second.

UDP - (User Datagram Protocol):One of the protocols for data transfer that is part of the *TCP/IP* suite of protocols. UDP is a "stateless" protocol in that UDP makes no provision for acknowledgement of packets received.

Unix: A computer operating system (the basic software running on a computer, underneath things like word processors and spreadsheets). Unix is designed to be used by many people at the same time (it is multi-user) and has *TCP/IP* built-in. It is the most common operating system for *servers* on the *Internet*.

Upload: Transferring data (usually a file) from a computer you are using to another computer. The opposite of *download*.

URI - (Uniform Resource Identifier): An address for s resource available on the Internet. The first part of a URI is called the "scheme". the most well known scheme is *http*, but there are many others. Each URI scheme has its own format for how a URI should appear.

URL - (Uniform Resource Locator): The term URL is basically synonymous with *URI*. URI has replaced URL in technical specifications.

URN - (Uniform Resource Name): A *URI* that is supposed to be available for along time. For an address to be a URN some institution is supposed to make a commitment to keep the resource available at that address.

USENET: A world-wide system of discussion groups, with comments passed among hundreds of thousands of machines. Not all USENET machines are on the *Internet*. USENET is completely decentralized, with over 10,000 discussion areas, called *newsgroups*.

UUENCODE - (Unix to Unix Encoding):A method for converting files from *Binary* to *ASCII* (text) so that they can be sent across the Internet via *email*.

Veronica- (Very Easy Rodent Oriented Net-wide Index to Computerized Archives): Developed at the University of Nevada, Veronica was a constantly updated database of the names of almost every menu item on thousands of *gopher* servers. The Veronica database could be searched from most major *gopher* menus. Now made obsolete by web-bases search engines.

Virus: A chunk of computer programming code that makes copies of itself without any conscious human intervention. Some viruses do more than simply replicate themselves, they might display messages, install other software or files, delete software of files, etc.

VOIP - (Voice Over IP): A specification and various technologies used to allow making telephone calls over *IP* networks, especially the *Internet*. Just as *modems* allow computers to connect to the Internet over regular telephone lines, VOIP technology allows humans to talk over Internet connections. Costs for VOIP calls can be a lot lower than for traditional telephone calls. Because the IP networks are *packet-switched* this allows for vastly different ways of handling connections and more efficient use of network resources.

VPN - (Virtual Private Network):Usually refers to a *network* in which some of the parts are connected using the public *Internet*, but the data sent across the Internet is encrypted, so the entire network is "virtually" private.

WAIS - (Wide Area Information Servers):Developed in the early 1990s WAIS was the first truly large-scale system to allow the indexing of huge quantities of information on the *Web*, and to make those indices searchable across *networks* such as the *Internet*. WAIS was also pioneering in its use of ranked (scored) results where the software tries to determine how relevant each result it.

WAN - (Wide Area Network):Any *internet* or *network* that covers an area larger than a single building or campus.

WebDAV - (Web-based Distributed Authoring and Versioning):A set of extensions to the *HTTP* protocol that allows multiple users to not only read but also to add, delete, and change documents residing on a web server. In order to use WebDAV you need WebDAV *client* software to connect to a HTTP *server* that has the WebDAV extensions installed.

Wi-Fi - (Wireless Fidelity): A popular term for a form of wireless data communication, basically Wi-Fi is "Wireless Ethernet".

Wiki: A wiki is a web site for which the content can be easily edited and altered from the web browser in which you are viewing it. Typically there is an "edit" button on each page and the wiki is configured to allow either anyone or only people with passwords to edit each page. The word "wiki" comes from a Hawaiian word meaning "quick."

Worm: A worm is a *virus* that does not infect other programs. It makes copies of itself, and infects additional computers (typically by making use of network connections) but does not attach itself to additional programs; however, a worm might alter, install, or destroy files and programs.

XHTML - (eXtensible HyperText Markup Language): Basically *HTML* expressed as valid *XML*. XHTML is intended to be used in the same places you would use HTML (creating web pages) but is much more strictly defined, which makes it a lot easier to create software that can read it, edit it, check it for errors, etc. XHTML is expected to eventually replace HTML.

XML - (eXtensible Markup Language):A widely used system for defining data formats. XML provides a very rich system to define complex documents and data structures such as invoices, molecular data, news feeds, glossaries, inventory descriptions, real estate properties, etc. As long as a programmer has the XML definition for a collection of data (often called a "schema") then they can create a program to reliably process any data formatted according to those rules.

XMLRPC - (XML Remote Procedure Call): A *protocol* for *client-server* communication that sends and receives information "on top of" *HTTP*. The data sent and received is in a particular *XML* format specifically designed for use with XMLRPC.

XPFE - (Cross Platform Front End): A suite of technologies used to create applications that will work and look the same on different computer operating systems. A widely used XPFE application is the Mozilla web browser and its derivatives, such as the Netscape web browser in version 7 and later. The primary technologies used in creating XPFE applications are *Javascript*, *Cascading Style Sheets*, and *XUL*.

XUL- (eXtensible User-interface Language) :A markup language similar to *HTML* and based on *XML*. XUL used to define what the user interface will look like for a particular piece of software. XUL is used to define what buttons, scrollbars, text boxes, and other user-interface items will appear, but it is not used to define how that item will look (e.g. what color they are). The most widely used example of XUL use is probably in the Firefox web browser, where the entire user interface is defined using the XUL language.

Post Quiz Answers

Topic 1 Answers – 1. File Transfer Protocol, 2. Human-Machine Interface, 3. Industrial Control System, 4. Local Area Network, 5. True, 6. False, 7. True, 8. True, 9. Architecture, 10. Data acquisition, 11. ALARM or NORMAL, 12. Alarm activation, 13. RTU, 14. Hot standby or dual-redundant formation, 15. Supervisory computer

Topic 2 Answers- 1. False, 2. False, 3. True, 4. True, 5. False, 6. True, 7. False, 8. False, 9. True, 10. Data historian, 11. PLCs, RTUs and IEDs, 12. An IO server, 13. Fieldbus technologies, 14. Control network, 15. Remote access points

Topic 3- Answers -1. False, 2. True, 3. False, 4. True, 5. True, 6. Access control, 7. Upgrade, 8. Communication protocols, 9. 3-5, 10. 15-20, 11. Defense-in-depth strategy, 12. Vulnerabilities, 13. Cornerstone, 14. Connections to the ICS, 15. Worms and other malware

Topic 4 Answers - 1. ICS, 2. Cyber security management program, 3. Interconnectivity, 4. DoS attacks, 5. Security, 6. Compliance, 7. Architecture to procurement, 8. Applications, 9. Vulnerability assessment, 10. An accidental DoS, 11. Devices and networks, 12. IT system, 13. An IT system, 14. Real-world consequences, 15. Longevity

Topic 5- Answers – 1. Corporate network, 2. Security and performance, 3. DMZ, 4. Separate network segment, 5. ICS, 6. Ports, 7. Network firewalls, 8. TCP/IP protocol suite, 9. Unauthorized access, 10. Corporate, 11. Security, 12. ICS, 13. An intermediate DMZ, 14. Architectures, 15. Data historian

Topic 6 – Answers – 1. True, 2. False, 3. False, 4. True, 5. False, 6. False, 7. False, 8. False, 9. True, 10. True, 11. False, 12. False, 13. False, 14. True, 15. True

Appendix C—Current Activities in Industrial Control System Security

This appendix contains abstracts of some of the many activities that are currently addressing industrial control system cyber security. Please be aware that organization descriptions and related information provided in this appendix has been drawn primarily from the listed organizations' Web sites and from other reliable public sources, but has not been verified. Readers are encouraged to contact the organizations directly for the most up-to-date and complete information.

American Gas Association (AGA) Standard 12, "Cryptographic Protection of SCADA Communications"

Standard 12 Documents: **http://gtiservices.org/security/aga12_wkgdoc_homepg.shtml**
American Gas Association: **http://www.aga.org/**
The American Gas Association, representing 195 local energy utility organizations that deliver natural gas to more than 56 million homes, businesses, and industries throughout the United States, advocates the interests of its energy utility members and their customers, and provides information and services. The AGA 12 series of documents recommends practices designed to protect SCADA communications against cyber incidents. The recommended practices focus on ensuring the confidentiality of SCADA communications. The document series, "Cryptographic Protection of SCADA Communications", when complete will consist of the following four documents:

- **AGA 12-1** Background, Policies and Test Plan
- **AGA 12-2** Retrofit Link Encryption for Asynchronous Serial Communications
- **AGA 12-3** Protection of Networked Systems
- **AGA 12-4** Protection Embedded in SCADA Components.

The purpose of the AGA 12 series is to save SCADA system owners' time and effort by recommending a comprehensive system designed specifically to protect SCADA communications using cryptography. The AGA 12 series may be applied to water, wastewater, and electric SCADA-based distribution systems because of their similarities with gas systems, however timing requirements may be different. Recommendations included in the series 12 documents may also apply to other ICS. Additional topics planned for future addendums in this series include key management, protection of data at rest, and security policies.

American Petroleum Institute (API) Standard 1164, "Pipeline SCADA Security"

API Standard 1164: **http://api-ep.api.org/filelibrary/1164PA.pdf**
American Petroleum Institute: **http://api-ec.api.org/**
The American Petroleum Institute represents more than 400 members involved in all aspects of the oil and natural gas industry. API 1164 provides guidance to the operators of oil and gas liquid pipeline systems for managing SCADA system integrity and security. The guideline is specifically designed to provide operators with a description of industry practices in SCADA security, and to provide the framework needed to develop sound security practices within the operator's individual organizations.

It stresses the importance of operators understanding system vulnerability and risks when reviewing the SCADA system for possible system improvements. API 1164 provides a means to improve the security of SCADA pipeline operations by:

- Listing the processes used to identify and analyze the SCADA system's susceptibility to incidents
- Providing a comprehensive list of practices to harden the core architecture

 Providing examples of industry best practices.

The standard targets small to medium pipeline operators with limited IT security resources. The standard is applicable to most SCADA systems, not just oil and gas SCADA systems. The appendices of the document include a checklist for assessing a SCADA system and an example of a SCADA control system security plan.

Center for Control System Security at Sandia National Laboratories (SNL)

http://www.sandia.gov/scada/

The Center for Control System Security is composed of several test bed facilities, which allow real-world critical infrastructure problems to be modeled, designed, simulated, verified, and validated. These labs are integrated into a research effort focusing on solving current control system security problems and developing next generation control systems. These facilities include the following:

- **Distributed Energy Technology Laboratory (DETL)**, which provides a platform to test the control of operational generation and load systems
- **Network Laboratory**, which provides network visualization and wired and wireless network modeling
- **Cryptographic Research Facility**, which supports research and development of encryption for applications in control system networks
- **Red Team Facility**, which provides a suite of tools to attack and analyze control system vulnerabilities
- **Advanced Information Systems Lab**, which is used to research intelligent technologies for development of the infrastructures of the future.

Chemical Industry Data Exchange (CIDX)

http://www.cidx.org/

CIDX is a trade association and standards body whose mission is to improve the ease, speed, and cost of conducting business electronically between chemical organizations and their trading partners.

A cyber security initiative within CIDX is working to establish management practices, procedures, guidelines, and standards to support overall chemical sector cyber security. The group is also working with service providers, government, and academia to accelerate the development of affordable security technology solutions. CIDX has developed several documents relating to cyber security and the chemical sector that are available on their Web site at http://www.cidx.org/CyberSecurity/publications/default.asp.

CIDX has established the Cyber-Security Practices, Standards and Technology Initiative to identify immediate opportunities to improve the base level of cyber security within the chemical industry. The objective of this initiative is to address the practices and standards for both business systems and control systems.

DHS Control Systems Security Program (CSSP)

http://www.uscert.gov/control_systems/

To reduce control systems vulnerabilities, the DHS National Cyber Security Division (NCSD) established the Control Systems Security Program (CSSP) and the US-CERT Control Systems Security Center (CSSC). The CSSP coordinates efforts among federal, state, and local governments, as well as control system owners, operators, and vendors to improve control system security within and across all critical infrastructure sectors by reducing cyber security vulnerabilities and risk. The US-CERT CSSC coordinates control system incident management, provides timely situational awareness information, and manages control system vulnerability and threat reduction activities.

The NCSD has established a strategy to guide the partnership between government and industry to improve the security posture of control systems within the nation's critical infrastructure. The strategy incorporates five highly integrated goals to address the issues associated with control systems security:

- Facilitate the US-CERT capability to coordinate control system incident management, provide timely situational awareness information for control systems, and manage control system vulnerability and threat reduction activities.
- Organize and coordinate national resources to create a center of excellence that provides a proactive environment for vulnerability reduction, security assessments, and risk analysis.
- Enhance industry practices for securing control systems against cyber-attacks by providing tools to assess the security posture of control system operating environments and recommending measures for mitigation of vulnerabilities.
- Enhance control systems security awareness and promote a self-sustaining security culture within the control systems community through participation in working groups, standards development bodies, and user conferences to build cooperative and trusted relationships and enhance control systems security efforts.
- Make strategic recommendations as to the development and testing of next-generation secure control systems and security products.

DHS CSSP Recommended Practices

http://csrp.inl.gov/

The DHS Control Systems Security Program (CSSP) Recommended Practices site provides a current information resource to help industry understand and prepare for ongoing and emerging control systems cyber security issues, vulnerabilities and mitigation strategies.

The CSSP works with the control systems community to ensure that recommended practices, which are made available, have been vetted by subject-matter experts in industry before being made publicly available in support of this program.

Recommended practices are developed to help users reduce their exposure and susceptibility to cyber-attacks. These recommendations are based on understanding the cyber threats, control systems vulnerabilities and attack paths, and control systems engineering. The initial practices recommended by the working group detail Defense in Depth and Mitigations for Control System Vulnerabilities of a secure architecture. More topics are slated for addition on a continuing basis. Additional supporting documents that cover specific issues and associated mitigations are also included on this site. This site will continue to evolve and grow as new recommended practices and related information are added.

DHS Process Control Systems Forum (PCSF)

https://www.pcsforum.org/

The purpose of the PCSF is to accelerate the design, development, and deployment of more secure new and legacy control systems. PCSF participants include international stakeholders from government; academia; industry users, owner/operators, and systems integrators; and the vendor community. The PCSF is an open, collaborative, voluntary forum that will leverage and unify the experience, capabilities, and contributions of these stakeholders through meetings, interest groups, and working groups, to develop and adopt common architectures, protocols, and practices.

The PCSF is funded by Department of Homeland Security/Homeland Security Advanced Research Projects Agency (DHS/HSARPA) and managed by Mitretek Systems. It is not a standards body and is not intended to replace any existing activities in the SCADA and ICS security community.

Rather, it will build upon the existing body of work and establish links with others in industry and government, to arrive at a common underlying architecture for process control systems that offers security, reliability, resiliency, and continuity in the face of disruptions and major incidents. The PCSF encourages the active participation of individuals interested in advancing security and reliability in process control systems.

The PCSF is a forum for the control systems community that is uniquely positioned to:

- Aggregate information about current organizations and their efforts, directions, and work products from across multiple sectors to increase visibility and reduce redundancy
- Identify consensus cross-industry and cross-functional issues that require resolution, and determine a path and effort that is owned, traceable, and produces generally acceptable solutions
- Cross-connect decision-makers from industry, government, vendors, and academia in ways that promote increased understanding of requirements and opportunities for collaboration
- Impact a broad portion of the control system community through procedures, methods, guidelines, best practices, and other resources, issued through organizations that participate in the PCSF.

International Electrotechnical Commission (IEC) Technical Committees 65 and 57
http://www.iec.ch/

IEC is a standards organization that prepares and publishes international standards for all electrical, electronic, and related technologies. These standards serve as a basis for creating national standards and as references for drafting international tenders and contracts. IEC's members include manufacturers, providers, distributors, vendors, consumers, users, all levels of governmental agencies, professional societies, trade associations, and standards developers from over 60 countries.

In 2004 the IEC Technical Sub-Committee 65C (Digital Communications), through its working group WG13 (Cyber Security), started to address security issues - within the IEC 61784 standard – for field buses and other industrial communication networks. Results of this work are outlined in part 4, entitled "Digital data communications for measurement and control – Profiles for secure communications in industrial networks".

TC65 WG10 is working to extend this field level communication to address security standards across common automation networking scenarios. The standard being drafted as a result of this work is IEC 62443, entitled "Security for industrial process measurement and control – Network and system security". It is based on a modular security architecture consisting of requirement sets. These modules are mapped into ICS component and network architecture. The resulting requirements can then be formulated for use as the basis for Requests for Proposals (RFP) for data communication standards, and security audits.

TC 57 is focused on Power Systems Management and Associated Information Exchange and is divided up into a series of working groups. Each working group is comprised of members of national standards committees from the countries that participate in the IEC. Each working group is responsible for the development of standards within its domain.

The current working groups are:
- WG 3: Telecontrol protocols
- WG 7: Telecontrol protocols compatible with ISO Standards and ITU-T recommendations
- WG 9: Distribution automation using distribution line carrier systems
- WG 10: Power system IED communication and associated data models
- WG 13: Energy management system application program interface
- W14: System interfaces for distribution management
- WG 15: Data and communication security
- WG 16: Deregulated energy market communications
- WG 17: Communications systems for distributed energy resources
- WG 18: Hydroelectric power plants – communication for monitoring and control
- WG 19: Interoperability within TC 57 in the long term

ISA-SP99 Manufacturing and Control Systems Security Standards

http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821

The ISA-SP99 Committee is establishing standards, recommended practices, technical reports, and related information that will define procedures for implementing electronically secure industrial automation and control systems and security practices and assessing electronic security performance.

Guidance is directed toward those responsible for designing, implementing, or managing industrial automation and control systems and shall also apply to users, system integrators, security practitioners, and control system manufacturers and vendors.

The committee's focus is to improve the confidentiality, integrity, and availability of components or systems used for manufacturing or control and provide criteria for procuring and implementing secure control systems. Compliance with the committee's guidance will improve manufacturing and control system electronic security, and will help identify vulnerabilities and address them, thereby reducing the risk of compromising confidential information or causing industrial automation control system degradation or failure. There are several planned standards in the ISA-99 series. Each will cover a specific aspect or subset of the subject of industrial automation and control systems security.

They are:

- **ISA 99.00.01 Concepts, Models and Terminology:** defines the basic concepts and terminology that form the basis for the remaining standards in the SP99 series so that all readers of the standard will operate on a common framework
- **ISA 99.00.02 Establishing an Industrial Automation and Control Systems Security Program:** provides a basic guidebook that an implementer of the SP99 standard can use to assemble a security program, without prescribing the details for every industry type
- **ISA 99.00.03 Operating an Industrial Automation and Control Systems Security Program:** describes how to run a security program after it is designed and implemented
- **ISA 99.00.04 Specific Security Requirements for Industrial Automation and Control Systems:** defines the characteristics of manufacturing and control systems that differentiate them from other IT systems from a security point of view. Based on these characteristics, it establishes the security requirements that are unique to this class of system.

SP99's first efforts resulted in two Technical Reports that are now available from ISA as ANSI/ISA-TR99.00.01 - Application and Practices, and ANSI/ISA-TR99.00.02 - Integrating Electronic Security into the Manufacturing and Control Systems Environment.

ISA-SP100 Wireless Systems for Automation

http://www.isa.org/MSTemplate.cfm?MicrositeID=1134&CommitteeID=6891

The ISA-SP100 Committee will establish standards, recommended practices, technical reports, and related information that will define procedures for implementing wireless systems in the automation and control environment with a focus on the field level. Guidance is directed towards those responsible for the complete life cycle including the designing, implementing, on-going maintenance, scalability or managing manufacturing and control systems, and shall apply to users, system integrators, practitioners, and control systems manufacturers and vendors.

ISO 17799 Security Techniques – Code of Practice for Information Security Management

http://www.iso.org/

ISO 17799 provides guidelines and voluntary directions for information security management. It addresses topics in terms of policies and general good practices. The document specifically identifies itself as “a starting point for developing organization specific guidance”. It states that not all of the guidance and controls it contains may be applicable and that additional controls not contained may be required. It is not intended to give definitive details or “how-to’s”. Given such caveats, the document briefly addresses the following major topics:

- Organizational security policy
- Organizational security infrastructure
- Asset classification and control
- Personnel security
- Physical and environmental security
- Communications and operations management
- Access control
- Systems development and maintenance
- Business continuity management
- Compliance.

ISO 17799 is transitioning to the new ISO 27000 series. In the near future ISO 17799 will become ISO 27002. (http://www.27000.org/)

International Council on Large Electric Systems (CIGRE)

http://www.cigre.org/

The International Council on Large Electric Systems (CIGRE) is a nonprofit international association based in France. It has established several study committees to promote and facilitate the international exchange of knowledge in the electrical industry by identifying best practices and developing recommendations. Three of its study committees focus on control systems:

- The objectives of the Substations Committee include the adoption of technological advances in equipment and systems to achieve increased reliability and availability.
- The System Operation and Control Committee focuses on the technical capabilities needed for the secure and economical operation of existing power systems including control centers and operators.
- The Information Systems and Telecommunication for Power Systems Committee monitors emerging technologies in the industry and evaluates their possible impact. In addition, it focuses on the security requirements of the information systems and services of control systems.

LOGI^{2}C – Linking the Oil and Gas Industry to Improve Cyber Security

http://www.hsarpacyber.com/logic.html

LOGI^{2}C is a 12-month technology integration and demonstration project jointly supported by industry partners and the U.S. Department of Homeland Security (DHS). The project demonstrates an opportunity to reduce vulnerabilities of oil and gas process control environments by sensing, correlating and analyzing abnormal events to identify and prevent cyber security threats.

Motivation

The Process Control Networks and SCADA systems used by the Oil & Gas Industry are facing new threats and vulnerabilities. New threats come from terrorists who want to destabilize energy industry supply capabilities and the national economy. New vulnerabilities have been introduced with the migration to standard IT components (e.g. general-purpose computing platforms and standard operating systems), introduction of standard networking technology such as TCP/IP and Ethernet in the SCADA environment, and integration of business and process control networks.

Approach

This project intends to examine needs and solutions for correlating and analyzing abnormal events to provide indications and warnings of cyber-security threats. The end vision is to enable informed response to threats by taking corrective action. The goal of the project is to achieve the ability to correlate abnormal events from the process control network and its interfaces to the corporate network with alerts from sources on the corporate network (intrusion detection systems, firewalls, etc.). The project partners will:

- Identify new types of security sensors for process control networks
- Adapt a best-of-breed correlation engine to this environment
- Integrate in test bed and demonstrate
- Transfer technology to field operations

Organization

LOGI^{2}C is an example of a partnership between Government and Industry. In this project, the oil and gas companies contribute the operational environment and expertise, and project management, while the vendor companies provide security expertise and products. DHS Science and Technology Directorate contributes testing facilities and independent research staff with technical security expertise.

National Infrastructure Simulation and Analysis Center (NISAC)

http://www.lanl.gov/orgs/chs/biip/nisac.shtml

NISAC, a joint program between Los Alamos National Laboratory and Sandia National Laboratories**,** is providing modeling, simulation, and analysis of critical infrastructures, their interdependencies, complexities, and the potential consequences of disruptions. Such tools are important for policy, planning (including evaluation of mitigation options), crisis response, and education and training. The models and tools address interdependency issues and questions at a national or regional scale, as well as at the urban or metropolitan level. The capabilities being developed as part of NISAC will be of value to other organizations in DHS such as the Undersecretary for Emergency Preparedness and Response, and the Department of Energy/Office of Energy Assurance.

National SCADA Test Bed (NSTB)

http://www.inl.gov/scada/factsheets/d/nstb.pdf

The DOE Office of Electricity Delivery and Energy Reliability (OE) seeks to improve the security and reliability of our Nation's energy delivery systems. OE established the National SCADA Test Bed (NSTB) to help the energy sector and equipment vendors assess control system vulnerabilities and test the security of control systems hardware and software. Working in partnership with the energy sector, the National SCADA Test Bed seeks to:

- Identify and mitigate existing vulnerabilities.
- Facilitate development of security standards.
- Serve as an independent entity to test SCADA systems and related control system technologies.
- Identify and promote best cyber security practices.
- Increase awareness of control systems security within the energy sector.
- Develop advanced control system architectures and technologies that are more secure and robust.

Partners in the NSTB include Idaho National Laboratory, Sandia National Laboratories, Argonne National Laboratory, Pacific Northwest National Laboratory, and the National Institute of Standards and Technology.

NIST 800 Series Security Guidelines

http://csrc.nist.gov/publications/nistpubs/index.html

The NIST Special Publication 800 information technology series of documents reports on the NIST Information Technology Laboratory (ITL) research, guidance, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations. Focus areas include cryptographic technology and applications, advanced authentication, public key infrastructure, internetworking security, criteria and assurance, and security management and support. In addition to this publication, NIST SP 800-82, the following is a listing of some additional 800 series documents that have significant relevance to the ICS security community. These as well as many others are available through the URL listed above.

- NIST SP 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems*
- NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*
- NIST SP 800-40 Version 2, *Creating a Patch and Vulnerability Management Program*
- NIST SP 800-41, *Guidelines on Firewalls and Firewall Policy*
- NIST SP 800-42, *Guideline on Network Security Testing*
- NIST SP 800-48, *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*
- NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*
- NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*
- NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*
- NIST SP 800-61, *Computer Security Incident Handling Guide*
- NIST SP 800-63, *Electronic Authentication Guideline*
- NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle*
- NIST SP 800-70, *Security Configuration Checklists Program for IT Products—Guidance for Checklists Users and Developers*
- NIST SP 800-77, *Guide to IPSec VPNs*
- NIST SP 800-83, *Guide to Malware Incident Prevention and Handling*
- NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*
- NIST SP 800-88, *Guidelines for Media Sanitization*
- NIST SP 800-92, *Guide to Computer Security Log Management*
- NIST SP 800-94, *Guide to Intrusion Detection and Prevention (IDP) Systems*
- NIST SP 880-97, *Guide to IEEE 802.11i: Robust Security Networks*

NIST Industrial Control System Security Project

http://csrc.nist.gov/sec-cert/ics/index.html

Because today's ICSs are often a combination of legacy systems, often with a planned life span of twenty to thirty years, or a hybrid of legacy systems augmented with newer hardware and software that are interconnected to other systems, it is often difficult or infeasible to apply some of the security controls contained in NIST SP 800-53. Recognizing this problem, NIST has initiated a high-priority project in cooperation with the public and private sector ICS community to develop specific guidance on the application of the security controls in NIST SP 800-53 to ICSs.

NIST Industrial Control Security Testbed

http://www.isd.mel.nist.gov/projects/processcontrol/testbed.html

This is a laboratory scale testbed comprised of several implementations of typical industrial control and networking equipment as well as relevant sensors and actuators. This testbed is being used to develop performance metrics and tests that can be applied to industrial control security products to determine if particular time-sensitive requirements can be met. These performance metrics pertain to real-time requirements for data transfer, such as minimal delay and timing jitter, and are not considered in traditional IT networks. Work being performed on this testbed includes the development of metrics and tests to evaluate the performance of industrial networking equipment as well as the development of tests for evaluating the effects of security implementations on the operation of industrial control systems.

North American Electric Reliability Council (NERC)

http://www.nerc.com/

Designated by DOE as the electricity sector's information sharing and analysis center (ISAC) coordinator for CIP, the North American Electric Reliability Council (NERC) receives security data from the electricity sector; analyzes the data with input from DHS, other federal agencies, and other critical infrastructure sector ISACs; and disseminates threat indications, analyses, and warnings. NERC has also formed the Critical Infrastructure Protection Advisory Group (CIPAG), which guides security activities and conducts security workshops to raise the awareness of cyber and physical security in the electricity sector. A Process Control Systems Security Task Force within CIPAG specifically addresses the security of electricity control systems.

NERC is in the process of issuing cyber security standards to reduce the risk of compromise to electrical generation resources and high-voltage transmission systems above 35kV, also referred to as bulk electric systems. Bulk electric systems include Balancing Authorities, Reliability Coordinators, Interchange Authorities, Transmission Providers, Transmission Owners, Transmission Operators, Generation Owners, Generation Operators, and Load Serving Entities. The cyber security standards include audit measures and levels of non-compliance that can be tied to penalties.

The set of NERC Cyber Security Standards includes the following:

- CIP-002 Critical Cyber Assets
- CIP-003 Security Management Controls
- CIP-004 Personnel and Training
- CIP-005 Electronic Security
- CIP-006 Physical Security
- CIP-007 Systems Security Management
- CIP-008 Incident Reporting and Response Planning
- CIP-009 Recovery Planning.

Process Control Security Requirements Forum (PCSRF)

http://www.isd.mel.nist.gov/projects/processcontrol/

PCSRF was assembled to address the security requirements for industrial process control systems and components. NIST formed the Process Control Security Requirements Forum (PCSRF) in the spring of 2001. The NIST-led PCSRF is a working group of users, vendors, and integrators in the process control industry, which is addressing the cyber security requirements for new industrial process control systems and components, including SCADA systems, DCSs, PLCs, RTUs, and IEDs. Members of the PCSRF represent the critical infrastructures and related process industries, including oil and gas, water, electric power, chemicals, pharmaceuticals, metals and mining, and pulp and paper. There are currently over 700 members from 32 countries in the PCSRF representing the government, academic, and private sectors.

The main goal of the PCSRF is to increase the security of industrial process control systems through the definition and application of a common set of information security requirements for these systems. PCSRF has adopted the Common Criteria for Information Technology Security Evaluation, also known as ISO/IEC 15408, to document the results of this effort in the form of protection profile (PP) security specifications.

To date, the PCSRF has completed a baseline protection profile and is currently working to develop two PPs for the two major subsystems of a SCADA system, a Control Center PP and a Field Device PP.

- **System Protection Profile for Industrial Control Systems (SPP-ICS).** This completed document is designed to present a cohesive, cross-industry, baseline set of security requirements for industrial control systems. The SPP-ICS considers an entire system and addresses requirements for the entire system lifecycle. The SPP-ICS also acts as a starting point for more specific system protection profiles for a specific instance of an industrial control system, such as a DCS or a SCADA system, and for sub-systems such as control centers and field devices.
- **SCADA Protection Profile.** A SCADA PP is currently being developed using the SPP-ICC as a baseline to the effort. The SCADA PP is being developed as two individual PPs based on the two major subsystems of a SCADA system, a Control Center PP and a Field Device PP.

Inquiries for PCSRF PP development activities still in progress can be made through the PCSRF Web site.

SCADA and Control Systems Procurement Project

http://www.cscic.state.ny.us/msisac/scada/

The SCADA Procurement Project, established in March 2006, is a joint effort among public and private sectors focused on development of common procurement language that can be used by everyone. The goal is for federal, state and local asset owners and regulators to come together using these procurement requirements and to maximize the collective buying power to help ensure that security is integrated into SCADA systems.

US-CERT Control Systems Security Center (CSSC)

http://www.uscert.gov/control_systems/

The Control Systems Security Center (CSSC) is a state-of-the-art analysis and testing facility that works to provide proactive means for securing the control systems that operate many of the nation's critical infrastructures. It is managed by the Idaho National Laboratory (INL) for the Department of Homeland Security's (DHS) National Cyber Security Division (NCSD) and includes the participation of other DOE laboratories including Pacific Northwest, Los Alamos, Argonne, Sandia, and Savannah River. CSSC is tasked to identify technology gaps and operational security needs related to control system security and report these to DHS Science & Technology on areas of consideration for developmental efforts.

The CSSC performs its work through industry outreach, assessment and analysis, vulnerability testing, and awareness and response modeling. INL works together with industry and vendor manufacturers to assess current vulnerabilities and develop tools to secure them. The testing facility consists of functioning control systems from national and international manufacturers, a multi-functional cyber security testbed that is capable of performing cyber incidents and mock scenarios on various control systems, and an operational green room used for training and emergency management response.

Currently, the INL has working relationships established with over 30 utility organizations and equipment manufacturers. Awareness and response efforts provide continuous support to the United States Computer Emergency Readiness Team (US-CERT). All emergency requests related to control system security are forwarded to the US-CERT Support for Tier II response.

The National SCADA Testbed (NSTB) program is funded by the Department of Energy, while the CSSC is funded by the Department of Homeland Security. Both programs use the same facilities and testbeds, and many of the same personnel. The NSTB program is focused on reducing vulnerabilities of the electrical sector, while the CSSC program is concerned with all of the critical infrastructures in the United States.

Appendix D—Emerging Security Capabilities

This section provides an overview of security capabilities that are available to or being developed in support of the ICS community. There are several security products that are marketed specifically for ICS, while others are general IT security products that are being used with ICS. Many of the products available offer “single point solutions”, where a single security product offers multiple levels of protection. In addition to available products, this section also discusses some research and development work towards new products and technologies.

Encryption
Encryption protects the confidentiality of data by encoding the data to ensure that only the intended recipient can decode it. There are some commercially available encryption products designed specifically for ICS applications, as well as general encryption products that support basic serial and Ethernet-based communications.

In addition to these products, the ICS SCADA community is working to develop a standard for implementing the encryption of SCADA communications. The American Gas Association is working to develop a standard, AGA-12, *Cryptographic Protection of SCADA Communications*, to protect SCADA master-slave communication links from a variety of active and passive cyber-attacks by developing a set of standards to secure serial communication links using encryption. The AGA effort is broken into four parts, with each addressing different aspects of SCADA communication protection:

- AGA 12-1 summarizes cyber security policies, the background of the cyber security problem, and a procedure for testing cryptographic protection systems.
- AGA 12-2 is a detailed technical specification for building interoperable cryptographic modules to protect SCADA communications for low-speed legacy SCADA systems and dial-up maintenance ports.
- AGA 12-3 will describe how to protect high-speed SCADA communications over networked systems.
- AGA 12-4 will describe how to build next-generation SCADA systems with embedded AGA 12 compatible cryptography.

Because of the long life of SCADA systems, a decision was made to focus initial efforts on the protection of legacy systems. This decision has led to the near completion of parts 1 and 2, while parts 3 and 4 are still in the planning stages. Currently, AGA 12-1 has passed balloting procedures and AGA 12-2 has undergone laboratory testing and is now being field-tested. There are also plans for a large-scale pilot test to further validate the standard. In addition, national laboratories are conducting performance and security tests on the protocol, and organizations are producing prototype encryption modules. Efforts are also underway to develop conformance test procedures to evaluate these new products.

Firewalls
Firewalls are commonly used to segregate networks to protect and isolate ICSs. These implementations use commercially available firewalls that are focused on Internet and corporate application layer protocols and are not equipped to handle ICS protocols. The ICS community is investigating the possibility of adding protocol awareness to filtering devices. Research was performed by an IT security vendor in 2003 to develop a Modbus-based firewall: a netfilter/iptables extension that allows policy decisions to be made on Modbus/TCP header values just as traditional firewalls filter on TCP/UDP ports and IP addresses [78]. However, to date no commercial product has been released with a Modbus firewall capability.

Intrusion Detection and Prevention
Intrusion detection systems (IDS) and intrusion prevention systems (IPS) are being deployed on ICS networks and components to detect well-known cyber-attacks. Network IDS products monitor network traffic and use various detection methods, such as comparing portions of the traffic to signatures of known attacks. In contrast, host intrusion detection uses software loaded on a host computer, often with attack signatures, to monitor ongoing events and data on a computer system for possible exploits. IPS products take intrusion detection a step further by automatically acting on detected exploits to attempt to stop them [58].

The required task of a security team to constantly monitor, evaluate, and quickly respond to intrusion detection events is sometimes contracted to a managed security service provider (MSSP). MSSPs have correlation and analysis engines to process and reduce the vast amounts of events logged per day to a small subset that needs to be manually evaluated. There are also correlation and analysis engine products available to large organizations wanting to perform this function in-house. Security information and event management (SIEM) products are used in some organizations to monitor, analyze, and correlate events from IDS and IPS logs, as well as audit logs from other computer systems, applications, infrastructure equipment, and other hardware and software, to look for intrusion attempts.

Current IDS and IPS products are effective in detecting and preventing many well-known Internet attacks, but until recently they have not addressed ICS protocol attacks. IDS and IPS vendors are beginning to develop and incorporate attack signatures for various ICS protocols such as Modbus, DNP, and ICCP. One cooperative effort within the ICS community is developing Snort rules for Modbus TCP, DNP3, and ICCP.

Snort is an open source network intrusion detection and prevention system using a rule-driven language to perform signature, protocol, and anomaly-based inspections. The current rule sets, covering Modbus, DNP, and ICCP, are basic, and efforts are underway to expand them. The rules are available at no cost to any ICS user, vendor, integrator, or consultant [60]. The documentation, test data, and configuration files are also available for free. This same industry group is also defining a data dictionary of log entries from various ICS applications. The data dictionary helps cyber security monitoring products and services identify and understand the meaning of security events in ICS application logs using normalized events. The dictionary is still under development. Some commercial IDS and IPS vendors are also offering some ICS protocol signatures. [59].

As with any software added to an ICS component, the addition of host IDS or IPS software could affect system performance. IPSs are commonplace in today’s information security industry, but can be very resource intensive.

These systems have the ability to automatically reconfigure systems if an intrusion attempt is identified. This automated and fast reaction is designed to prevent successful exploits; however, an automated tool such as this could be used by an adversary to adversely affect the operation on an ICS by shutting down segments of a network or server. False positives can also hinder ICS operation.

Malware/Antivirus Software

Because early malware threats were primarily viruses, the software to detect and remove malware has historically been called “antivirus software”, even though it can detect many types of malware. Antivirus software is used to counter the threats of malware by evaluating files on a computer’s storage devices (some tools also detect malware in real-time at the network perimeter and/or on the user’s workstation) against an inventory of malware signature files. If one of the files on a computer matches the profile of known malware, the malware is removed through a disinfection process so it cannot infect other local files or communicate across a network to infect other files on other computers. There are also techniques available to identify unknown malware “in-the-wild” when a signature file is not yet available.

Many end-users and vendors of ICSs are recommending the use of COTS antivirus software with their systems and have even developed installation and configuration guidance based on their own laboratory testing. Some ICS vendors recommend the use of antivirus software with their products, but offer little to no guidance. Some end users and vendors are hesitant to use antivirus software due to fears that its use would cause ICS performance problems or even failure. NIST and Sandia National Laboratories (SNL) are conducting a study and producing a report aimed at helping ICS owners/operators to deploy antivirus software and to minimize and assess performance impacts of workstation and server-based antivirus products. This study has assembled a vast amount of ICS-based antivirus knowledge into a single document, which serves as a starting point or a secondary resource when installing, configuring, running, and maintaining antivirus software on an ICS [57]. In many cases, performance impacts can be reduced through configuration settings as well as antivirus scanning and maintenance scheduling outside of the antivirus software practices recommended for typical IT systems. This cooperative industry effort has also made antivirus software vendors more aware of ICS and their special performance requirements, initiating better communications within the two fields.

In summary, COTS antivirus software can be used successfully on most ICS components. However, special ICS specific considerations should be taken into account during the selection, installation, configuration, operational, and maintenance procedures. ICS end-users should consult with the ICS vendors regarding the use of antivirus software and can also use the output of the NIST and SNL study as supplemental information.

Vulnerability and Penetration Testing Tools

There are many tools available for performing network vulnerability assessments and penetration tests for ICSs; however, the impacts these tools may have on the operation of an ICS should be carefully considered[79]. The additional traffic and exploits used during active vulnerability and penetration testing, combined with the limited resources of many ICSs, have been known to cause ICSs to malfunction. As guidance in this area, SNL has developed a preferred list of vulnerability and penetration testing techniques for ICS [79]. These are less intrusive methods, passive instead of active, to collect the majority of information that is often queried by automated vulnerability and penetration testing tools. These methods are intended to allow collection of the necessary vulnerability information without the risk of causing a failure while testing.

ICS owners must make the individuals using vulnerability and penetration testing tools aware of the criticality of continuous operation and the risks involved with performing these tests on operational systems. It may be possible to mitigate these risks by performing tests on ICS components such as redundant servers or independent test systems in a laboratory setting. Laboratory tests can be used to screen out test procedures that might harm the operational system.

Even with very good configuration management to assure that the test system is highly representative, tests on the actual system are likely to uncover flaws not represented in the laboratory.

Appendix E—Industrial Control Systems in the FISMA Paradigm

In recognition of the importance of information security to the economic and national interests of the United States, the Federal Information Security Management Act (FISMA) [13] was established to require each Federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency. The NIST FISMA Implementation Project [14] was established in January 2003 to produce several key security standards and guidelines required by Congressional legislation including:

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

Key FISMA-related publications include Federal Information Processing Standards (FIPS) 199, FIPS 200, and NIST SPs 800-18, 800-30, 800-37, 800-53, 800-53A, 800-59 and 800-60. A specific guidance document on the application of the FIPS risk framework and its supporting documentation for ICSs is scheduled for release at the beginning of fiscal year 2007 and may be added as an Appendix to this document.

Below is a listing of NIST FIPS and SPs documenting these standards and guidelines.21

FIPS Publication 199: Standards for Security Categorization of Federal Information and Information Systems contains standards to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels [15]. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization resulting from the operation of its information systems.

FIPS Publication 200: Minimum Security Requirements for Federal Information and Information Systems specifies minimum security requirements for information and information systems supporting the executive agencies of the Federal government and a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements [16]. The document provides links to NIST SP 800-53 (*Recommended Security Controls for Federal Information Systems*), which recommends management, operational, and technical controls needed to protect the confidentiality, integrity, and availability of all Federal information systems that are not national security systems.

NIST SP 800-18: Guide for Developing Security Plans for Information Systems contains guidelines to develop, document, and implement an agency-wide information security program that includes subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems [17].

NIST SP 800-30: Risk Management Guide for Information Technology Systems has guidelines to develop an agency-wide information security program that includes periodic assessment of the risk and magnitude of the harm that could result from unauthorized access, use disclosure, disruption, modifications, or destruction of information and information systems [19].

NIST SP 800-37: Guide for the Security Certification and Accreditation of Federal Information Systems provides guidance on conducting periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices (including management, operational, and technical security controls) [20].

NIST SP 800-53: Recommended Security Controls for Federal Information Systems provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the Federal government [21]. The guidelines apply to all components of an information system that process, store, or transmit Federal information with the exception of systems designated as national security systems. A project is currently underway to provide guidance on the application of SP 800-53 in ICS, including the use of compensating controls to cover control that cannot technically be met in an ICS.

NIST SP 800-53A: Guide for Assessing Security Controls in Federal Information Systems provides guidance for conducting periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices (including management, operational, and technical security controls) [22].

NIST SP 800-59: Guideline for Identifying an Information System as a National Security System provides guidelines developed in conjunction with the Department of Defense, including the National Security Agency, for identifying an information system as a national security system [23].

NIST SP 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories presents guidelines that recommend the types of information and information systems to be included in each security category defined in FIPS 199 [24].

NIST SP 800-70: Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers discusses the development of security configuration checklists and option selections that minimize the security risks associated with commercial IT products used within the Federal government [25].22

This set of documents provides security standards and guidelines that support an enterprise-wide risk management process. The documents are intended to be an integral part of a Federal agency's overall information security program. Figure E-1 shows a diagram of this framework and the relevancy of supporting documents.

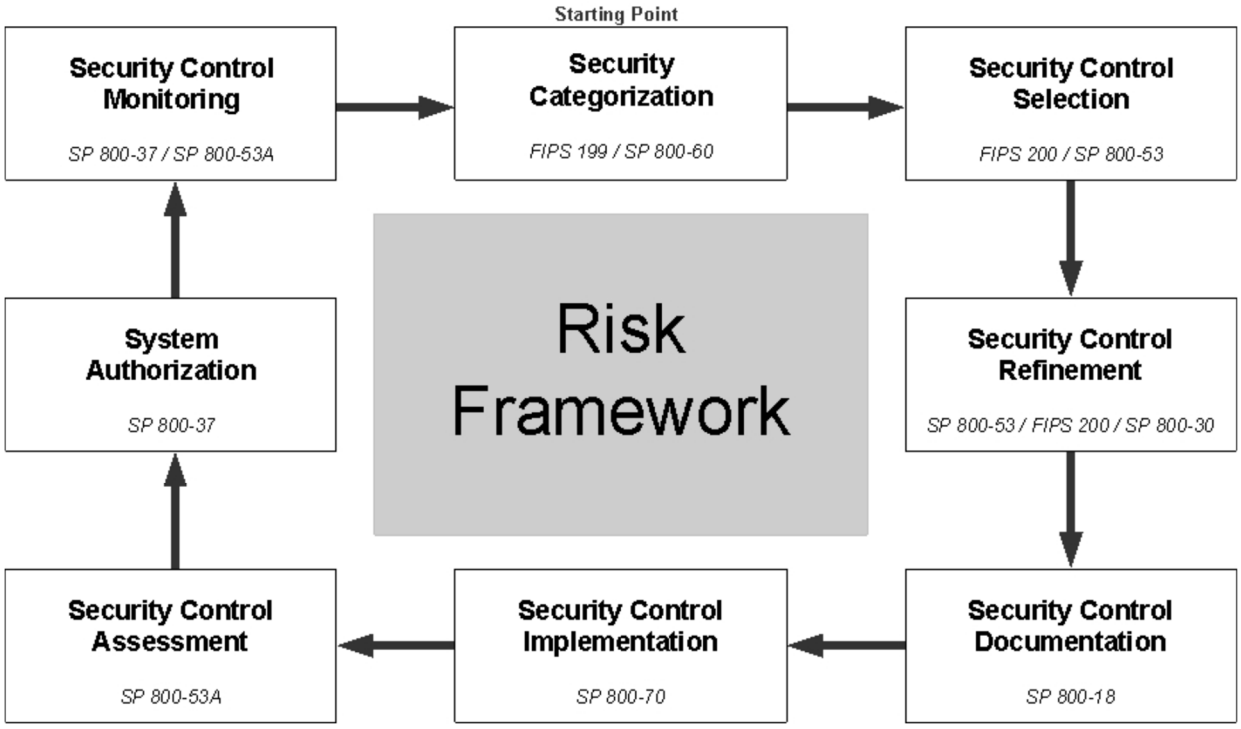


Figure E-1. Risk Framework

The following is a chronological listing of the Risk Framework activities, a description of each activity, and identification of supporting NIST documents. [26]

Security Categorization

The first activity in the Risk Framework is to categorize the information and information system according to potential impact of loss. For each information type and information system under consideration, the three FISMA defined security objectives—confidentiality, integrity, and availability—are associated with one of three levels of potential impact should there be a breach of security. It is important to remember that for an ICS, availability is generally the greatest concern.

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

$SC_{\text{information type or system}}$ = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)}, where the acceptable values for potential impact are LOW, MODERATE, or HIGH.

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

FIPS 199 establishes security categories for both information and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.

The security category of an information type can be associated with both user information and system information and can be applicable to information in either electronic or non-electronic form. It can also be used as input in considering the appropriate security category of an information system. Establishing an appropriate security category of an information type essentially requires determining the potential impact for each security objective associated with the particular information type.

Determining the security category of an information system requires slightly more analysis and must consider the security categories of all information types resident on the information system. For an information system, the potential impact values assigned to the respective security objectives (confidentiality, integrity, availability) are the highest values (i.e., high water mark) from among those security categories that have been determined for each type of information resident on the information system.

The following example is taken from FIPS 199:
A power plant contains a SCADA system controlling the distribution of electric power for a large military installation. The SCADA system contains both real-time sensor data and routine administrative information. The management at the power plant determines that: (i) for the sensor data being acquired by the SCADA system, there is no potential impact from a loss of confidentiality, a high potential impact from a loss of integrity, and a high potential impact from a loss of availability; and (ii) for the administrative information being processed by the system, there is a low potential impact from a loss of confidentiality, a low potential impact from a loss of integrity, and a low potential impact from a loss of availability.

The resulting security categories, SC, of these information types are expressed as:
SC sensor data = {(**confidentiality**, NA), (**integrity**, HIGH), (**availability**, HIGH)},
and

SC administrative information = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}.

The resulting security category of the information system is initially expressed as:
SC SCADA system = {(**confidentiality**, LOW), (**integrity**, HIGH), (**availability**, HIGH)},
representing the high water mark or maximum potential impact values for each security objective from the information types resident on the SCADA system.

The management at the power plant chooses to increase the potential impact from a loss of confidentiality from low to moderate, reflecting a more realistic view of the potential impact on the information system should there be a security breach due to the unauthorized disclosure of system-level information or processing functions. The final security category of the information system is expressed as:

SC SCADA system = {(**confidentiality**, MODERATE), (**integrity**, HIGH), (**availability**, HIGH)}.
FIPS 199 specifies that information systems be categorized as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. Possible definitions for low, moderate, and high levels of security based on impact for ICS based on ISA-TR99.00.02 [27] are provided in Table E-1.

Possible definitions for ICS impact levels based on product produced, industry and security concerns are provided in Table E-2.

Table E-1. Possible Definitions for ICS Impact Levels Based on ISA-TR99.00.02

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

Table E-2. Possible Definitions for ICS Impact Levels Based on Product Produced, Industry and Security Concerns

Category	Low-Impact	Moderate-Impact	High-Impact
Product Produced	• Non-hazardous materials or products • Non-ingested consumer products	• Some hazardous products or steps during production • High amount of proprietary information	• Critical infrastructure (e.g. electricity, etc.) • Hazardous materials • Ingested products
Industry Examples	• Plastic injection molding • Warehouse application s	• Automotive metal industries • Pulp and paper • Semiconductors	• Utilities • Petrochemical • Food and beverage • Pharmaceutical
Security Concerns	• Protection against minor injuries • Ensuring uptime	• Protection against moderate injuries • Ensuring uptime • Capital investment	• Protection against major injuries/loss of life • Ensuring uptime • Capital investment • Trade secrets • Ensuring basic social services • Regulatory compliance

Security Control Selection

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

The security-related areas are:

- Access Control (AC)
- Awareness and Training (AT)
- Audit and Accountability (AU)
- Certification, Accreditation, and Security Assessments (CA)
- Configuration Management (CM)
- Contingency Planning (CP)
- Identification and Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Physical and Environmental Protection (PE)
- Planning (PL)
- Personnel Security (PS)
- Risk Assessment (RA)
- System and Services Acquisition (SA)
- System and Communications Protection (SC)
- System and Information Integrity (SI).

To aid in selecting controls to meet these requirements, NIST SP 800-53 provides fundamental concepts and a process for selection and specification of security controls for an information system. Security controls are organized into classes and families for ease of use in the selection and specification process.

Each family name and unique control identifier corresponds to the above listing of minimum-security requirements. The families are divided among three classes: management, operational, and technical. Each security control within a family contains the following information:

Control – describes specific security related activities or actions to be carried out by the organization or the information system. The control selections often contain assignment and selection options for customizing a security control.

Supplemental Guidance – provides additional information related to a specific security control that should be considered when selecting and implementing security controls.

Control Enhancements – provides statements of security capability to add functionality to or increase the strength of a basic control.

Security Control Refinement

This activity performs a risk assessment to adjust minimum-security controls to local conditions, required threat coverage, and specific agency requirements. NIST SP 800-30 provides practical guidance for assessing and mitigating risks identified within information systems. The last section of Appendix E provides additional guidance on tailoring the minimum-security controls to address the specific requirements of ICS.

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

Security Control Implementation
This activity involves the implementation of security controls in new or legacy information systems. To help make this process consistent across the Federal government, NIST is currently working to develop security configuration checklists, which are documented sets of instructions for configuring products to pre-defined security baselines [28] (e.g., NIST SP 800-68*, Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist).*

Security Control Assessment
This activity determines the extent to which the security controls in the information system are effective in their application. NIST SP 800-53A provides guidance for assessing security controls initially selected from NIST SP 800-53 to ensure they are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the system.

To accomplish this, the document provides expectations based on assurance requirements defined in NIST SP 800-53 for characterizing the expectations of security assessments by FIPS 199 impact level.

NIST SP 800-53A also supports:
- FISMA annual assessments for major information systems
- Security certifications as part of formal system certification and accreditation processes
- Continuous monitoring of selected security controls
- Preparation for an audit
- Identification of resource needs to improve the system's security posture

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

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

Interim Guidance on the Application of Security Controls to ICS
Because today's ICSs are often a combination of legacy systems, often with a planned life span of twenty to thirty years, or a hybrid of legacy systems augmented with newer hardware and software that are interconnected to other systems, it is often difficult or infeasible to apply some of the security controls contained in NIST SP 800-53. Recognizing this problem, NIST has initiated a high-priority project23 in cooperation with the public and private sector ICS community to develop specific guidance on the application of the security controls in NIST SP 800-53 to ICSs. Since the project is still ongoing, the resulting guidance could not be included in the current release of this document or NIST SP 800-53.

However, based on the project results to date, NIST makes the following observations and recommendations for organizations that own and operate ICSs:

- Section 3.3 of NIST SP 800-53, *Tailoring the Initial Baseline*, allows the organization to modify or adjust the recommended security control baselines when certain conditions exist that require that flexibility. Based on the discussion above, NIST recommends that ICS owners take advantage of the ability to tailor the initial baselines when it is not possible or feasible to implement specific security controls contained in the baselines. However, all tailoring activity should, as its primary goal, focus on meeting the intent of the original security controls whenever possible or feasible.

- In some cases, it may be infeasible, impractical, or unsafe to implement a specific security control within an ICS. For example, AC-11, *Session Lock*, is required for all moderate impact and high impact information systems. For ICSs with requirements for real-time response and extremely high availability, predictability, and reliability, session lock may not make sense (e.g., locking an operator's session in an electric power distribution system or an air traffic control system). However, the purpose of the session lock control is to prevent unauthorized access to an information system when the user or operator leaves the terminal or workstation unattended for a period of time. In this case, to meet the intent of the session lock security control, an organization could utilize the compensating control concept described in Section 3.3 of NIST SP 800-53. With appropriate rationale and justification, an organization can choose to compensate for not using session locks by incorporating other safeguards and countermeasures, such as increasing physical security, ensuring physical isolation of the terminal or workstation, increasing personnel security, and/or adding surveillance equipment to ensure that only authorized or trusted personnel are permitted in the vicinity of the terminal or workstation.

Until NIST completes the ICS project and publishes specific guidance for ICSs, organizations should adjust their ongoing activities aimed at determining compliance with FIPS 200 and NIST SP 800-53 to allow for the types of flexibility that are discussed above. However, it is also reasonable to require ICS owners to develop a multi-year plan to demonstrate how the system owner plans to transition the ICS to a state that is fully compliant with FIPS 200 and NIST SP 800-53, particularly for systems that are planned to be in operation for several more years.

Section 6 summarizes the management, operational and technical controls identified in NIST SP 800-53, and provides initial guidance on how these security controls apply to ICSs. Initial recommendations and guidance, if available, will be provided in an outlined box for each section.

Appendix References

GUIDE TO SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) AND INDUSTRIAL CONTROL SYSTEMS SECURITY (DRAFT)

[56] Kent, Karen, and Mell, Peter, NIST SP 800-94, *Guide to Intrusion Detection and Prevention (IDP) Systems*, 2006, http://csrc.nist.gov/publications/drafts/Draft-SP800-94.pdf

[57] Falco, Joe, et al., *Using Anti-virus Software on Industrial Control Systems: Integration Guidance and a Test Methodology for Assessing Performance Impacts*, 2006, Draft Document, http://www.isd.mel.nist.gov/projects/processcontrol/AV_Guide_PCSF_Draft_Release_20060530.pdf

[58] Peterson, Dale, *Intrusion Detection and Cyber Security Monitoring of SCADA and DCS Networks*, ISA, 2004, http://www.digitalbond.com/SCADA_security/ISA%20Automation%20West.pdf.

[59] *Symantec Expands SCADA Protection for Electric Utilities*, http://www.symantec.com/about/news/release/article.jsp?prid=20050914_01

[60] Digital Bond, http://www.digitalbond.com/support-center/.

[61] Grance, Tim, et al., NIST SP 800-61, *Computer Security Incident Handling Guide*, 2004, http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf.

[62] Mell, Peter, et al., NIST SP 800-83, *Guide to Malware Incident Prevention and Handling*, 2005, http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf.

[63] Wilson, Mark, and Hash, Joan, NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, 2003, http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.

[64] Mix, S., *Supervisory Control and Data Acquisition (SCADA) Systems Security Guide*, EPRI, 2003.

[65] Karygiannis, Tom, and Owens, Les, NIST SP 800-48, *Wireless Network Security, 802.11, Bluetooth and Handheld Devices*, 2002, http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf.

[66] Frankel, Sheila, et al, NIST SP800-97 Draft, *Guide to IEEE 802.11i: Establishing Robust Security Networks*, 2006, http://csrc.nist.gov/publications/drafts/Draft-SP800-97.pdf

[67] Federal Information Processing Standards Publication: FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, NIST, 2006, http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

[68] Dray, James, et al, NIST SP 800-96, *PIV Card to Reader Interoperability Guidelines*, 2006, http://csrc.nist.gov/publications/nistpubs/800-96/SP800-96-091106.pdf

[69] Polk, W., Timothy, et al, NIST SP800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, 2005, http://csrc.nist.gov/publications/nistpubs/800-78/sp800-78-final.pdf

[70] Souppaya, Murugiah, Kent, Karen, NIST SP800-92, Guide to Computer Security Log Management, 2006, http://csrc.nist.gov/publications/drafts/DRAFT-SP800-92.pdf

[71] Jansen, Wayne, NIST SP 800-28, *Guidelines on Active Content and Mobile Code*, 2001, http://csrc.nist.gov/publications/nistpubs/800-28/sp800-28.pdf.

[72] Chernick, Michael, et al, NIST SP 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations, 2005, http://csrc.nist.gov/publications/nistpubs/800-52/SP800-52.pdf

[73] Barker, Elaine, et al., NIST SP 800-56, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, 2005, http://csrc.nist.gov/publications/drafts/SP800-56_7-5-05.pdf.
[74] Baker, Elaine, et al., NIST SP 800-57, Recommendation for Key Management, 2005, Part 1, General: http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part1.pdf, Part 2, Best Practices: http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part2.pdf.
[75] Kuhn, D. Richard, et al., NIST SP 800-58, *Security Recommendations for Voice Over IP Systems*, 2005, http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf.
[76] Frankel, Sheila, et al, NIST SP 800-77, *Guide to IPsec* VPNs, 2005, http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf.
[77] Internet Security Glossary: RFC 2828, http://rfc.net/rfc2828.html.
[78] Franz, Matthew, and Pothamsetty, Venkat, *ModbusFW Deep Packet Inspection for Industrial Ethernet*, Critical Infrastructure Assurance Group, Cisco Systems, 2004, http://www.scadasec.net/oldio/papers/franz-niscc-modbusfw-may04.pdf.
[79] Duggan, David, *Penetration Testing of Industrial Control Systems*, Report SAND2005-2846P, Sandia National Laboratories, 2005, http://www.sandia.gov/scada/documents/sand_2005_2846p.pdf.
[80] Kissel, Richard, et al., NIST SP 800-88, *Guidelines for Media Sanitization,* 2006, http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf.

We welcome you to complete the assignment in Microsoft Word. You can find the assignment at www.abctlc.com.

Once complete, just simply fax or e-mail the answer key along with the registration page to us and allow two weeks for grading.

Once we grade it, we will e-mail a certificate of completion to you.

Call us if you need any help. If you need your certificate back within 48 hours, you may be asked to pay a rush service fee of $50.00.

You can download the assignment in Microsoft Word from TLC's website under the Assignment Page. www.abctlc.com

You will have 90 days to successfully complete this assignment with a score of 70% or better. If you need any assistance, please contact TLC's Student Services.