Industrial Control System Security

NIST SP 800-82

NIST Industrial Control System
Cyber Security Workshop
23 October 2009

NIST SP 800-82

- Initial public draft released September 2006 - public comment period through December 2006
- Second public draft released September 2007 - public comment period through December 2007
- Final public draft released September 2008 - public comment period through December 2008
- Final document should be released by end of 2009
- Downloaded over **750,000** times since initial release and is heavily referenced by the industrial control community
- Current document available at:
  - http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf

NIST Special Publication 800-82: *Guide to Industrial Control Systems (ICS) Security*

Executive Summary

1. Introduction
2. Overview of Industrial Control Systems
3. ICS Characteristics, Threats and Vulnerabilities
4. ICS Security Program Development and Deployment
5. Network Architecture
6. ICS Security Controls

List of Appendices

Appendix A— Acronyms and Abbreviations

Appendix B— Glossary of Terms

Appendix C— Current Activities in Industrial Control System Security

Appendix D— Emerging Security Capabilities

Appendix E— Industrial Control Systems in the FISMA Paradigm

Appendix F— References

1. Introduction

1.1 Authority

1.2 Purpose and Scope

- Purpose: Provide guidance for establishing secure ICS, including implementation guidance for SP 800-53 controls
- Scope: SCADA, DCS, RTU, other control systems

1.3 Audience

- Control engineers, integrators and architects when designing and implementing secure SCADA and/or ICS
- System administrators, engineers and other IT professionals when administering, patching, securing SCADA and/or ICS
- Security consultants when performing security assessments of SCADA and/or ICS
- Managers responsible for SCADA and/or ICS
- Researchers and analysts who are trying to understand the unique security needs of SCADA and/or ICS
- Vendors developing products that will be deployed in SCADA and/or ICS

1.4 Document Structure

2. Overview of Industrial Control Systems

2.1 Overview of SCADA, DCS, and PLCs

2.2 ICS Operation

2.3 Key ICS Components

- 2.3.1 Control Components
- 2.3.2 Network Components

2.4 SCADA Systems

2.5 Distributed Control Systems

2.6 Programmable Logic Controllers

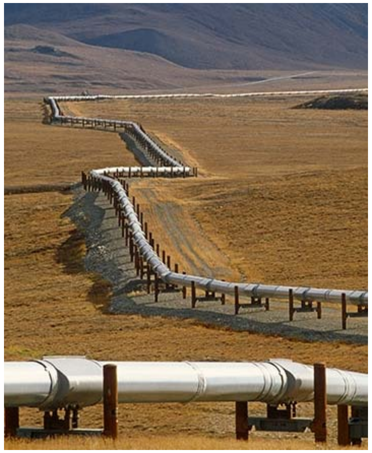
2.7 Industrial Sectors and Their Interdependencies

Industrial Control Systems (ICS)

- **Industrial Control System (ICS)** is a general term that encompasses several types of control systems including:
  - Supervisory Control and Data Acquisition (SCADA) systems
  - Distributed Control Systems (DCS)
  - Other control system configurations such as skid-mounted Programmable Logic Controllers (PLC)
- ICS are specialized Information Systems that physically interact with the environment
- Many ICS are components of the Critical Infrastructure

SCADA Examples

SCADA systems are used in the electricity sector, oil and gas pipelines, water utilities, transportation networks and other applications requiring remote monitoring and control.



Typical Control Room Layout

Control room provides network status, enables remote control, optimizes system performance, facilitates emergency operations, dispatching repair crews and coordination with other utilities.

Typical Operator Interface

Displays real-time network status on Geographic and schematic maps

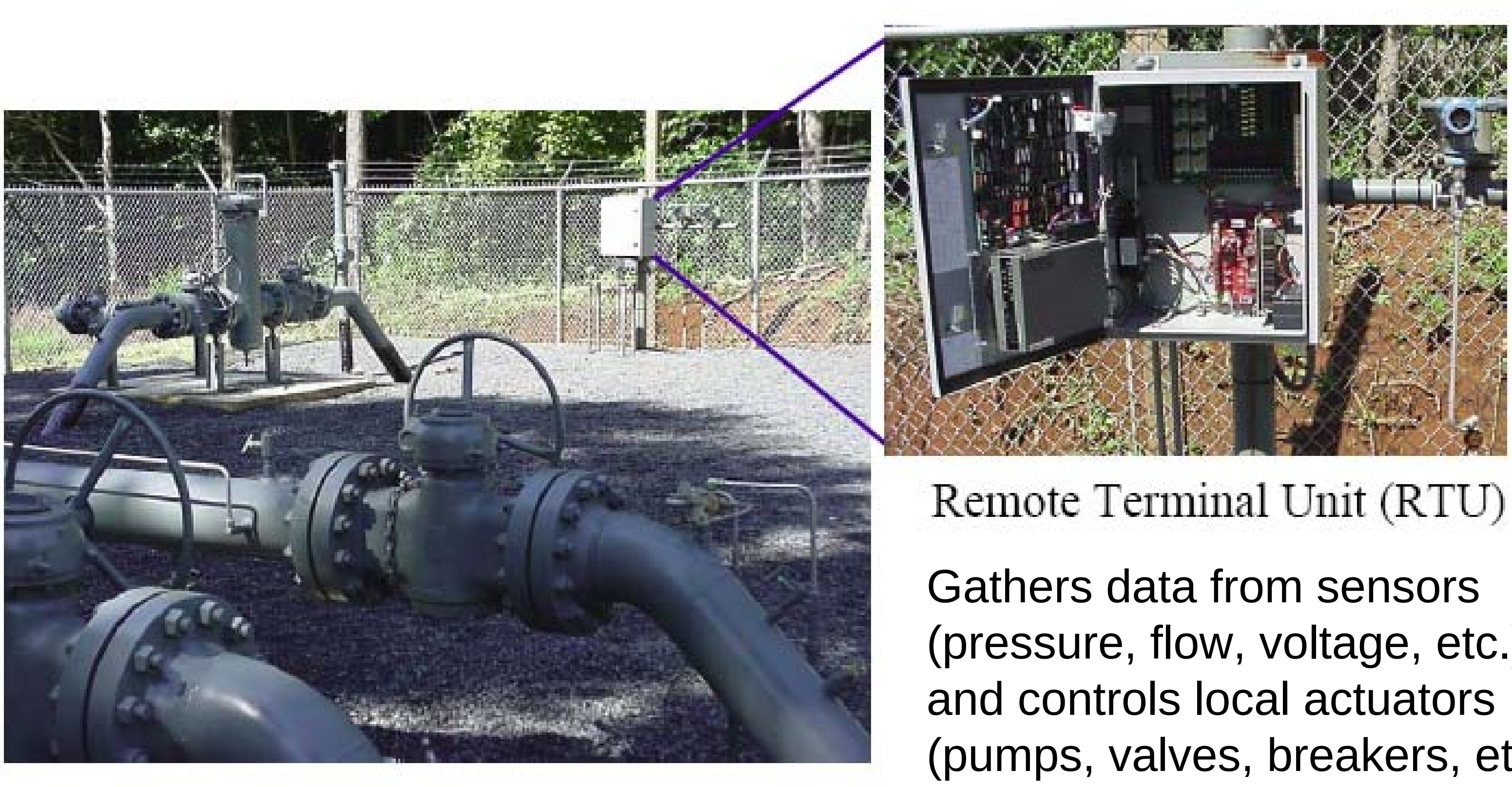
Provides control of circuit breakers, switches, etc.

Displays dynamic coloring to show real-time changes

Provides alarm status

Provides optimization functions and decision making support

Typical RTU Hardware



Remote Terminal Unit (RTU)

Gathers data from sensors (pressure, flow, voltage, etc.) and controls local actuators (pumps, valves, breakers, etc.)

DCS Examples

Electric Power Generation

Manufacturing

Refineries

3. ICS Characteristics, Threats and Vulnerabilities

3.1 Comparing ICS and IT Systems

3.2 Threats

3.3 Potential ICS Vulnerabilities

- 3.3.1 Policy and Procedure Vulnerabilities
- 3.3.2 Platform Vulnerabilities
- 3.3.3 Network Vulnerabilities

3.4 Risk Factors

- 3.4.1 Standardized Protocols and Technologies
- 3.4.2 Increased Connectivity
- 3.4.3 Insecure and Rogue Connections
- 3.4.4 Public Information

3.5 Possible Incident Scenarios

3.6 Sources of Incidents

3.7 Documented Incidents

Industrial Control System Security Challenges

- Real time constraints - IT security technology can impact timing, inhibit performance (response times are on the order of ms to s)
- Balancing of performance, reliability, flexibility, safety, security requirements
- Difficulty of specifying requirements and testing capabilities of complex systems in operational environments
- Security expertise and domain expertise required, but are often separated

Major ICS Security Objectives

- **Restricting logical access to the ICS network and network activity**
  - This includes using a demilitarized zone (DMZ) network architecture with firewalls to prevent network traffic from passing directly between the corporate and ICS networks, and having separate authentication mechanisms and credentials for users of the corporate and ICS networks. The ICS should also use a network topology that has multiple layers, with the most critical communications occurring in the most secure and reliable layer.
- **Restricting physical access to the ICS network and devices**
  - Unauthorized physical access to components could cause serious disruption of the ICS's functionality. A combination of physical access controls should be used, such as locks, card readers, and/or guards.

Major ICS Security Objectives (Cont.)

- **Protecting individual ICS components from exploitation**
    - This includes deploying security patches in as expeditious a manner as possible, after testing them under field conditions; disabling all unused ports and services; restricting ICS user privileges to only those that are required for each person's role; tracking and monitoring audit trails; and using security controls such as antivirus software and file integrity checking software where technically feasible to prevent, deter, detect, and mitigate malware.
- **Maintaining functionality during adverse conditions**
    - This involves designing the ICS so that each critical component has a redundant counterpart. Additionally, if a component fails, it should fail in a manner that does not generate unnecessary traffic on the ICS or other networks, or does not cause another problem elsewhere, such as a cascading event.

3.1 Comparing ICS and IT Systems

- **Performance Requirements**
- **Availability Requirements**
- **Risk Management Requirements**
- **Architecture Security Focus**
- **Physical Interaction**
- **Time-Critical Responses**
- **System Operation**
- **Resource Constraints**
- **Communications**
- **Change Management**
- **Managed Support**
- **Component Lifetime**
- **Access to Components**

Information Technology vs. Industrial Control Systems

Different Performance Requirements

Information Technology	Industrial Control
Non-Realtime	Realtime
Response must be reliable	Response is time critical
High throughput demanded	Modest throughput acceptable
High delay and jitter accepted	High delay and/or jitter is a serious concern

Information Technology vs. Industrial Control Systems

Different Reliability Requirements

Information Technology	Industrial Control
Scheduled operation	Continuous operation
Occasional failures tolerated	Outages intolerable
Beta testing in the field acceptable	Thorough testing expected

Information Technology vs. Industrial Control Systems

Different Risk Management Requirements: Delivery vs. Safety

Information Technology	Industrial Control
Data integrity paramount	Human safety paramount
Risk impact is loss of data, loss of business operations	Risk Impact is loss of life, equipment or product, environmental damage
Recover by reboot	Fault tolerance essential

These differences create huge differences in acceptable security practice

3.3.3 Network Vulnerabilities

Table 3-10. Network Perimeter Vulnerabilities

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

3.7 Documented Incidents

- Intentional Attacks
- Unintentional Consequences
  - External (to the organization)
  - Internal (to the organization)

Key Take Away to Securing ICS

The most successful method for securing an ICS is to:

- Gather industry recommended practices
- Engage in a ***proactive, collaborative effort*** between management, the controls engineer and operator, the IT department, the physical security department, and a trusted automation advisor
- Draw upon the wealth of information available from ongoing federal government, industry group, vendor and standards organizational activities.

4. ICS Security Program Development and Deployment

4.1 Business Case for Security

- 4.1.1 Benefits
- 4.1.2 Potential Consequences
- 4.1.3 Key Components of the Business Case
- 4.1.4 Resources for Building Business Case
- 4.1.5 Presenting the Business Case to Leadership

4.2 Developing a Comprehensive Security Program

- 4.2.1 Senior Management Buy-in
- 4.2.2 Build and Train a Cross-Functional Team
- 4.2.3 Define Charter and Scope
- 4.2.4 Define ICS Specific Security Policies and Procedures
- 4.2.5 Define and Inventory ICS Systems and Networks Assets
- 4.2.6 Perform Risk and Vulnerability Assessment
- 4.2.7 Define the Mitigation Controls
- 4.2.8 Provide Training and Raise Security Awareness

5. Network Architecture

5.1 Firewalls

5.2 Logically Separated Control Network

5.3 Network Segregation

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

5.3.2 Firewall between Corporate Network and Control Network

5.3.3 Firewall and Router between Corporate Network and Control Network

5.3.4 Firewall with DMZ between Corporate Network and Control Network

5.3.5 Paired Firewalls between Corporate Network and Control Network

5.3.6 Network Segregation Summary

5.4 Recommended Defense-in-Depth Architecture

5.5 General Firewall Policies for ICS

5.6 Recommended Firewall Rules for Specific Services

5.6.1 Domain Name System (DNS)

5.6.2 Hypertext Transfer Protocol (HTTP)

5.6.3 FTP and Trivial File Transfer Protocol (TFTP)

5.6.4 Telnet

5.6.5 Simple Mail Transfer Protocol (SMTP)

5.6.6 Simple Network Management Protocol (SNMP)

5.6.7 Distributed Component Object Model (DCOM)

5.6.8 SCADA and Industrial Protocols

5.7 Network Address Translation (NAT)

5.8 Specific ICS Firewall Issues

5.8.1 Data Historians

5.8.2 Remote Support Access

5.8.3 Multicast Traffic

5.9 Single Points of Failure

5.10 Redundancy and Fault Tolerance

5.11 Preventing Man-in-the-Middle Attacks

6. ICS Security Controls

(From SP 800-53 Control Families)

6.1 Management Controls

- 6.1.1 Risk Assessment
- 6.1.2 Planning
- 6.1.3 System and Services Acquisition
- 6.1.4 Certification, Accreditation, and Security Assessments
- 6.1.5 Program Management (New in SP 800-53, Rev 3)

6.2 Operational Controls

- 6.2.1 Personnel Security
- 6.2.2 Physical and Environmental Protection
- 6.2.3 Contingency Planning
- 6.2.4 Configuration Management
- 6.2.5 Maintenance
- 6.2.6 System and Information Integrity
- 6.2.7 Media Protection
- 6.2.8 Incident Response
- 6.2.9 Awareness and Training

6.3 Technical Controls

- 6.3.1 Identification and Authentication
- 6.3.2 Access Control
- 6.3.3 Audit and Accountability
- 6.3.4 System and Communications Protection

Control Family Sections

(Examples)

6.3 Technical Controls

- **Identification and Authentication (IA):** the process of verifying the identity of a user, process, or device, through the use of specific credentials (e.g., passwords, tokens, biometrics), 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.

Control Family Sections

(Examples continued)

6.3.1 Identification and Authentication

- **Description of I &A Family (in general IT sense)**
- **Supplemental Guidance**
  - 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**

  Systems in ICS environments typically rely on traditional passwords for authentication. Control system suppliers often supply systems with default passwords. These passwords are factory set and are often easy to guess or are changed infrequently, which creates additional security risks. Also, 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.

NIST Special Publication 800-82: *Guide to Industrial Control Systems (ICS) Security*

Executive Summary

1. Introduction
2. Overview of Industrial Control Systems
3. ICS Characteristics, Threats and Vulnerabilities
4. ICS Security Program Development and Deployment
5. Network Architecture
6. ICS Security Controls

List of Appendices

Appendix A— Acronyms and Abbreviations

Appendix B— Glossary of Terms

Appendix C— Current Activities in Industrial Control System Security

Appendix D— Emerging Security Capabilities

Appendix E— Industrial Control Systems in the FISMA Paradigm

Appendix F— References

Appendix C— Current Activities in Industrial Control System Security

- American Gas Association (AGA) Standard 12, “Cryptographic Protection of SCADA Communications”
- American Petroleum Institute (API) Standard 1164, “Pipeline SCADA Security”
- Center for Control System Security at Sandia National Laboratories (SNL)
- Chemical Sector Cyber Security Program
- Chemical Industry Data Exchange (CIDX)
- DHS Control Systems Security Program (CSSP)
- DHS CSSP Recommended Practices
- DHS Process Control Systems Forum (PCSF)
- Electric Power Research Institute (EPRI)
- Institute of Electrical and Electronics Engineers, Inc. (IEEE)
- Institute for Information Infrastructure Protection (I3P)
- International Electrotechnical Commission (IEC) Technical Committees 65 and 57
- ISA99 Industrial Automation and Control Systems Security Standards
- ISA100 Wireless Systems for Automation
- ISO 17799 Security Techniques – Code of Practice for Information Security Management
- ISO 27001 Information technology – Security techniques – Information security management systems – Requirements
- International Council on Large Electric Systems (CIGRE)
- LOGI2C – Linking the Oil and Gas Industry to Improve Cyber Security
- National SCADA Test Bed (NSTB)
- NIST 800 Series Security Guidelines
- NIST Industrial Control System Security Project
- NIST Industrial Control Security Testbed
- North American Electric Reliability Council (NERC)
- SCADA and Control Systems Procurement Project
- US-CERT Control Systems Security Center (CSSC)

Appendix D— Emerging Security Capabilities

- Encryption
- Firewalls
- Intrusion Detection and Prevention
- Malware/Antivirus Software
- Vulnerability and Penetration Testing Tools

Appendix E— Industrial Control Systems in the FISMA Paradigm

- FISMA Implementation Project Background (Ron)
- ICS Categorization Examples
- Applying 800-53 to ICS (Marshall)