# Supervisory Control and Data Acquisition (SCADA) Security

**Keith Stouffer**
**National Institute of Standards and Technology**

**Security Seminar for Critical Infrastructures**
**Kaiun Club, Hirakawa-cho, Chiyoda-ku, Tokyo**

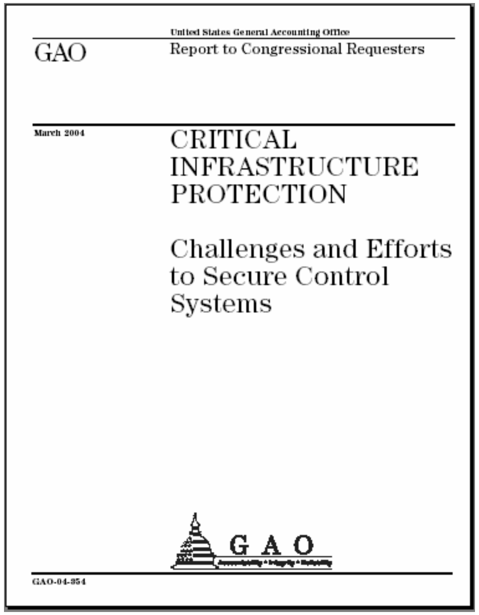
**February 14, 2007**

NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

ISD
Intelligent Systems Division
Manufacturing Engineering Laboratory

# Industrial Control System Security

- The (US) National Plan for Information Systems Protection and the recently released GAO-04-354 cite industrial control systems as critical points of vulnerability in America's utilities and industrial infrastructure... *"…Successful attacks on control systems could have devastating consequences, such as endangering public health and safety."*



United States General Accounting Office

GAO

Report to Congressional Requesters

March 2004

CRITICAL INFRASTRUCTURE PROTECTION

Challenges and Efforts to Secure Control Systems

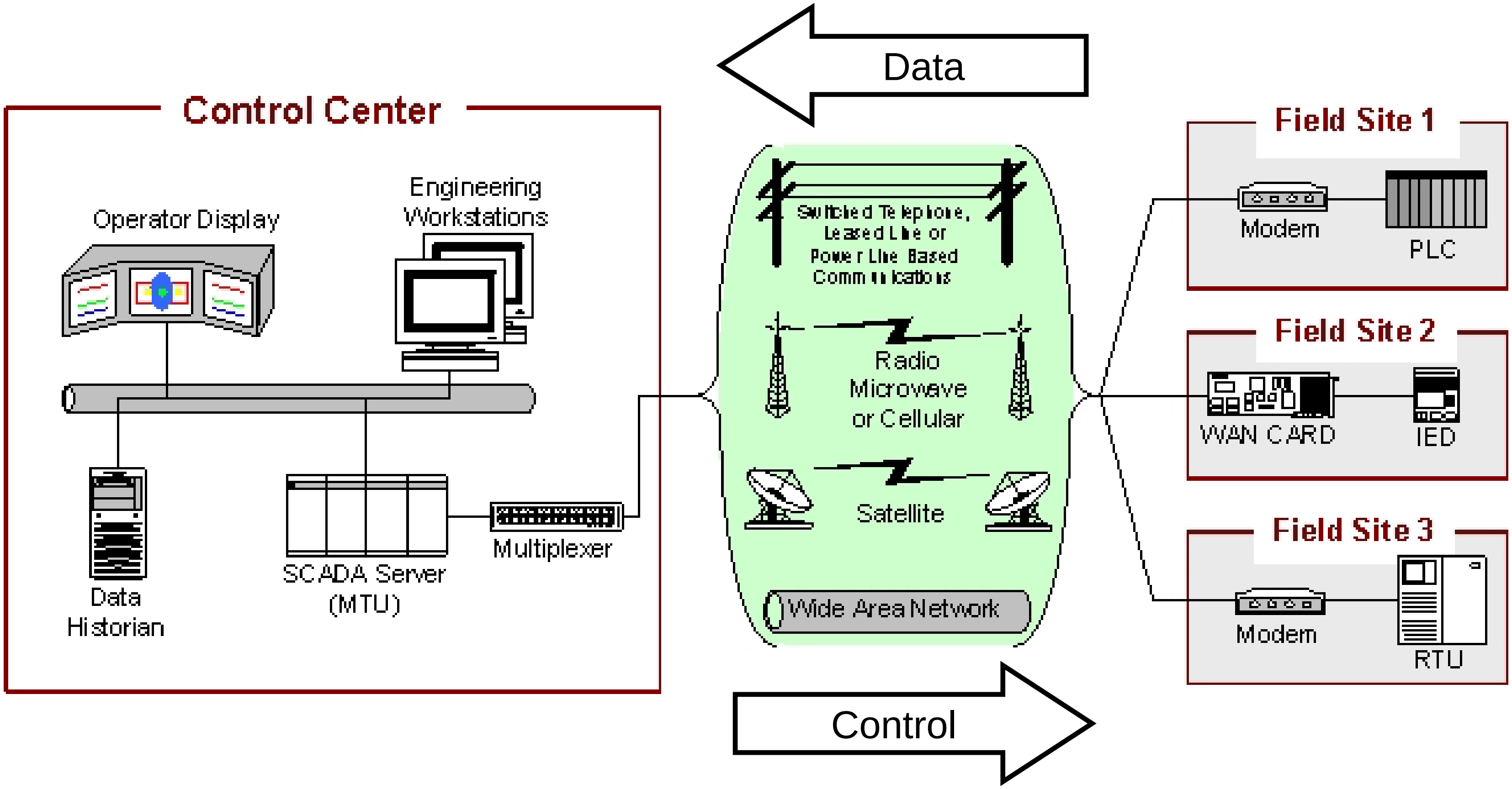
GAO

Accountability * Integrity * Reliability

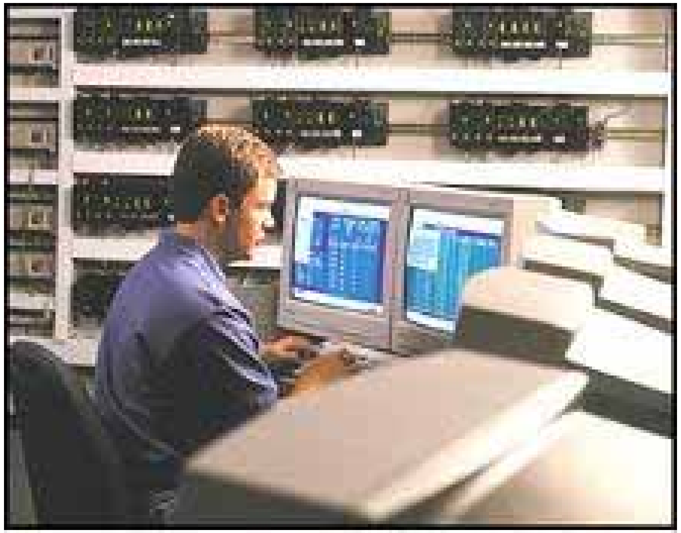
GAO-04-354

Electric power — Water — Oil & Gas
Transportation (rail, air, water, road)
Chemicals — Pharmaceuticals
Mining, Minerals & Metals
Pulp & Paper — Food & Beverage
Consumer Products
Discrete Manufacturing
(automotive, aerospace,
durable goods)

# General Supervisory Control and Data Acquisition (SCADA) System



# 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

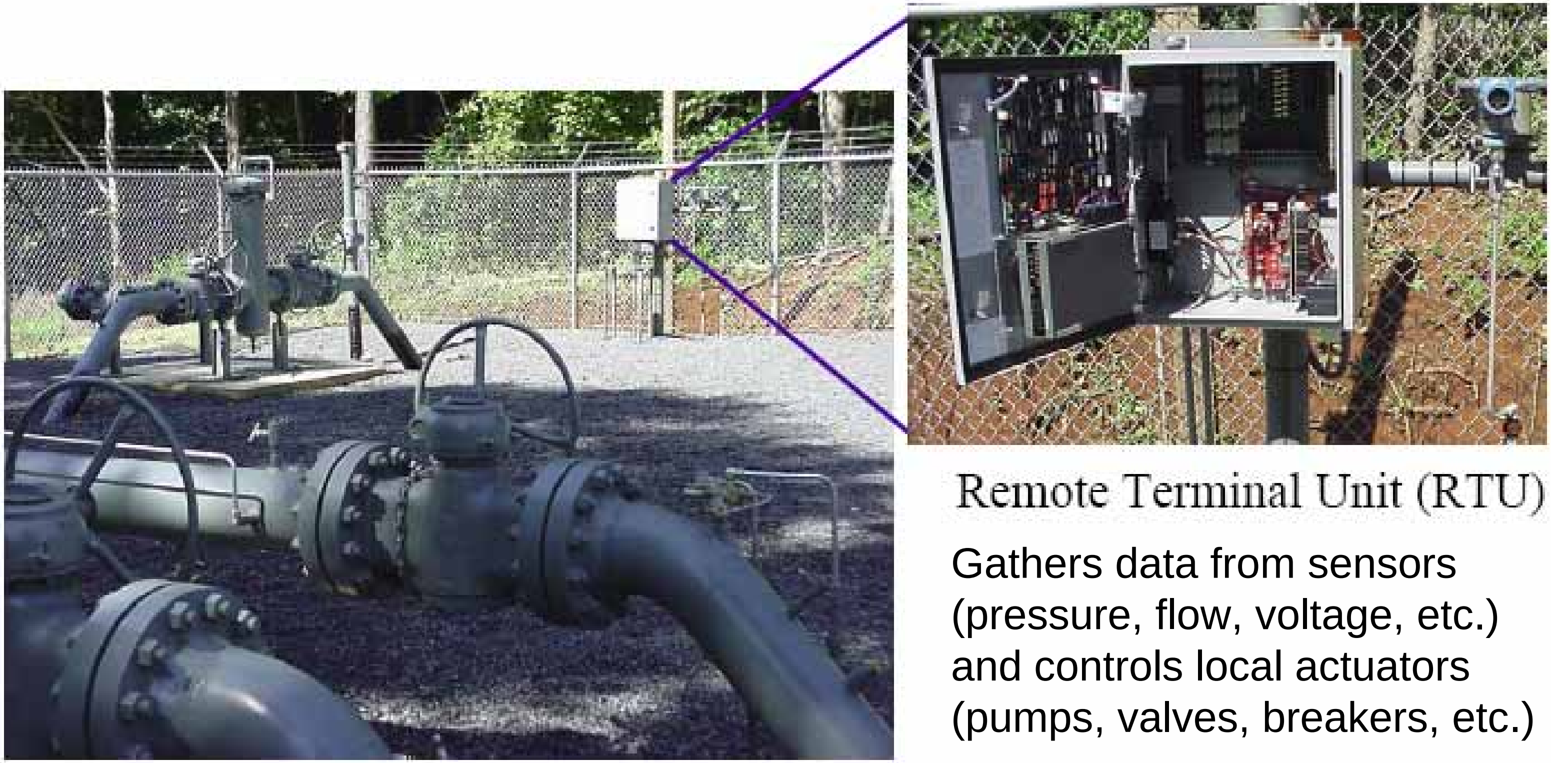
Provides control of circuit breakers, switches, etc.

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)

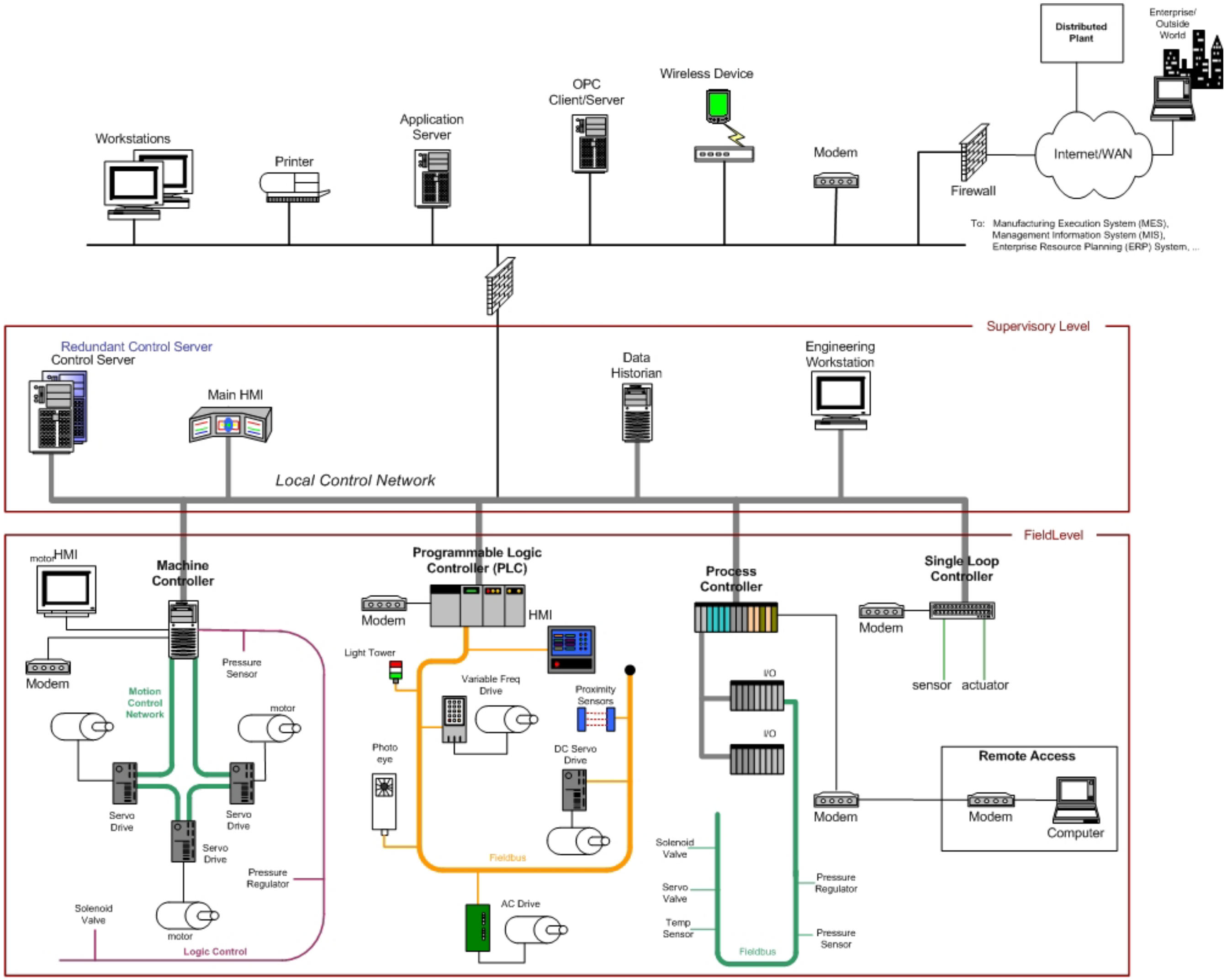
Gathers data from sensors (pressure, flow, voltage, etc.) and controls local actuators (pumps, valves, breakers, etc.)

# Typical IED Hardware

SEL-321
PHASE AND GROUND DISTANCE RELAY
DIRECTIONAL OVERCURRENT RELAY
FAULT LOCATOR
SEL
SCHWEITZER ENGINEERING LABORATORIES
WARNING

# Typical PLC Hardware

# General Distributed Control System (DCS)



# DCS Examples

Electric Power Generation

Manufacturing

Refineries

# Critical Infrastructure Protection

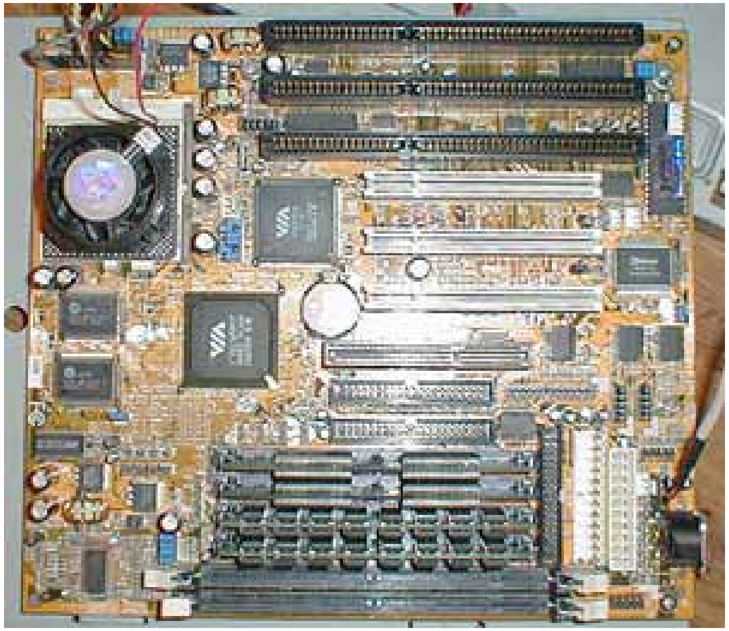
- In the U.S., the systems that control the critical infrastructures are over ***90%*** owned and operated by the private sector
- Critical infrastructure protection must be a ***partnership*** between the public and private sectors
- Information security solutions must be broad-based, consensus-driven, and address the ongoing needs of government and industry

# SCADA Trends

- Open Protocols
  - Open industry standard protocols are replacing vendor-specific proprietary communication protocols
- Interconnected to Other Systems
  - Connections to business and administrative networks to obtain productivity improvements and mandated open access information sharing
- Reliance on Public Information Systems
  - Increasing use of public telecommunication systems and the internet for portions of the control system

# Threats to Security

*Connectivity*



*Complexity*

# Adversaries

- **Unstructured adversaries**
    - Cracker, hacker, script-kiddie
    - Competitors
    - Criminals
- **Structured adversaries**
    - Terrorists, hactivists
    - Organized crime
    - Foreign nations
- **Insiders**
    - Witting
    - Unwitting

# Vulnerability Concerns

- **Confidentiality**
  - Protecting information from unauthorized access
  - Important for deregulation, competitive intelligence
- **Integrity**
  - Assuring valid data and control actions
  - Most critical for real-time control applications
- **Availability**
  - Continuity of operations
  - Important for real-time control applications
  - Historically addressed with redundancy

# Vulnerability Trends

- **Much more interconnectivity**
  - Internal and external networks merging
  - Functional, organization interconnection
- **Increased reliance on information systems**
  - Information becoming inseparable from the core business
- **Increased standardization**
  - Open protocols, common operating systems and platforms
- **Industry in transition**
  - Deregulation, mergers, new systems and procedures
  - Driven to “do more with less”

# Other Vulnerability Challenges

- Configuration management is not practiced beyond systems directly affecting physical operations
- Interconnectivity and interdependencies not widely understood
  - Boundaries of systems and authorities (particularly information systems) are becoming blurred
  - Level of trust granted is frequently unwarranted
  - Partitioning logical systems to control access and limit influence is not widely practiced
  - No explicit vendor security validation
- Limited incident detection, reporting, recovery, and forensics capability

# Typical Vulnerabilities Observed

- Ports and services open to outside
- Operating systems not “patched” with current releases
- Dial-up modems
- Improperly configured equipment (firewall does not guarantee protection)
- Improperly installed/configured software (e.g., default passwords)
- Inadequate physical protection
- Vulnerabilities related to “systems of systems” (component integration)

# The Global Threat

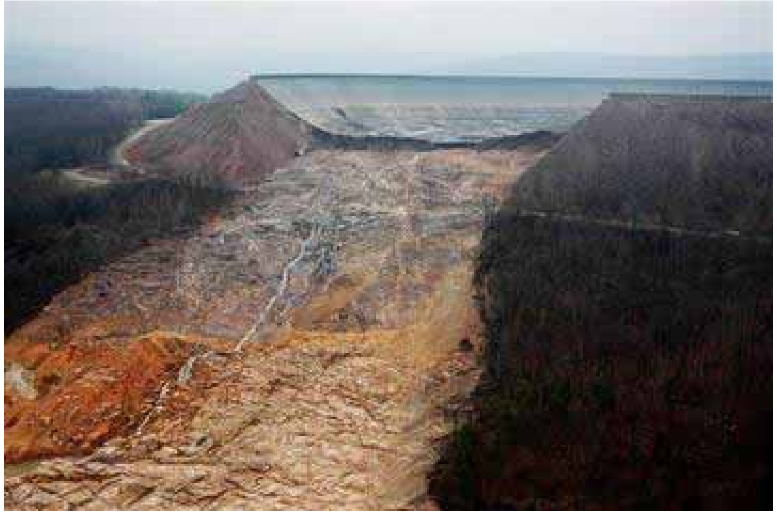
- Information security is not just a paperwork drill…there are dangerous adversaries out there capable of launching serious attacks on our information systems that can result in severe or catastrophic damage to the nation’s critical information infrastructure and ultimately threaten our economic and national security…
- Physical damage can result from control system anomalies – including intentional and unintentional events

# Gasoline Pipeline Failure

- **Event**: Gasoline pipeline failure exacerbated by control systems not able to perform control and monitoring functions
- **Industry**: Gasoline Pipeline
- **Location**: North America
- **Information Source**: NTSB Final Report
- **Impact**: 3 fatalities, total property damage >$45M
- **Lessons learned**:
  - Do not perform database update development while system in operation.
  - Apply appropriate security to remote access

# Water Storage Dam Failure

- **Event**: Remotely controlled Pumped Storage Dam Failure (Dec 14, 2005) due to instrument failure
- **Industry**: Hydro Storage Plant
- **Location**: North America
- **Information Source**: Utility & FERC
- **Impact**:
  - Loss of >450 MW hydro station
  - Environmental and economic loss still being evaluated
- **Lessons learned**:
  - Hardwired safety systems could prevent catastrophic events
  - Secure/Insure instrumentation



# 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

# 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 |
| Recover by reboot | Fault tolerance essential |

These differences create huge differences in acceptable security practice

# NIST Control System Security Program Summary

- **Goal:** To develop standards and test methods to enable the integration of security engineering into the industrial automation life cycle, including design, implementation, configuration, maintenance and decommissioning.
- **Outcome:** Reduced likelihood of successful cyberattack on the nation's critical infrastructure
- **NIST Role:** Working with federal and industry stakeholders to develop standards, guidelines, checklists, and test methods to help secure these critical control systems in harmony with their demanding safety and reliability requirements

# Process Control Security Requirements Forum (PCSRF)

Securing future systems:

Public/private partnership started in spring 2001 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.

Based on the *ISO 15408 Common Criteria for IT Security Evaluation*

# Collaborators/Partners

## Over 700 registered members including:

### ICS Vendors

ABB

Rockwell Automation

EMERSON

Wonderware

SIEMENS

Honeywell

GE FANUC

invensys

### IT Vendors

Cisco Systems

Sun microsystems

Microsoft

symantec.

### Standards Organizations

ISA — ISA-SP99

IEC — ISO/IEC 15408, 19791, 61508, 65C

AGA — AGA 12

### Government

Homeland Security

National Security Agency

DOE Labs

### End Users

GM

DU PONT

DOW

P&G

GP Georgia-Pacific

ALCOA

ChevronTexaco

ExxonMobil

# PCSRF Membership

http://www.isd.mel.nist.gov/projects/processcontrol

On 1/25/07 There were:

- 804 individual members from
- 436 organizations from
- 32 Countries (Australia, Austria, Belgium, Canada, Chile, China, Croatia, France, Germany, Hong Kong, India, Ireland, Israel, Italy, Japan, Lithuania, Netherlands, New Zealand, Norway, Panama, Portugal, Russia, Saudi Arabia, Singapore, South Africa, South Korea, Spain, Sweden, Switzerland, UK, USA, Venezuela)

# SP800-82 SCADA/ICS Security Guideline

- Guidance for establishing secure SCADA and Industrial Control Systems
- Provides an overview and presents typical topologies to facilitate the understanding of the unique security needs of industrial control systems
- Identifies typical vulnerabilities, threats and consequences
- Provides guidance on security deployment including administrative, physical and technical countermeasure to mitigate the associated risks
- First public draft available at: http://csrc.nist.gov/publications/drafts/800-82/Draft-SP800-82.pdf

# Defense in Depth Strategy

- Multiple layers of defense
  - Strong network perimeter
  - Perimeter intrusion detection
  - Internal access control to mission-critical systems
  - Internal intrusion detection
  - Host-level hardening of mission-critical systems
- Good configuration management
- Effective policies and procedures
- Security awareness, training, and management control

# Response and Recovery

- Contingency planning, disaster recovery drills
- Safety considerations
- Backup systems, restoration plans
- Preserve evidence
- Carefully evaluate system for changes
- Emphasizes the need for thorough and updated documentation, configuration management process

# Overarching Security Policy

- Establish high-level accountability
  - Spanning both physical and cyber security
- Develop security policies
  - Address security in the context of corporate goals
- Implement security procedures
  - Actual implementation, not just on paper
- Provide adequate training
  - General employees, system administrators, etc.
- Evaluate security in the context of an overarching risk management plan

# Other Issues

- Early detection is critical
  - Actively look for signs of malicious activity
  - Carefully evaluate trends, patterns
  - Notify appropriate authorities if malicious activity is detected
  - Ensure effective mechanisms are in place to follow-through
- Conduct periodic vulnerability assessments
  - Comprehensive, independent evaluation
  - Include penetration testing, active vulnerability scanning to identify and/or validate potential vulnerabilities
  - Engage broader elements of the organization

# Steps for Enhancing SCADA Security

- Establish a robust network architecture
- Eliminate trusted remote access points of entry
- Evaluate and deploy technology and approaches to enhance confidentiality, availability, and integrity
- Implement rigorous configuration management
- Provide adequate support and training
- Never become complacent!

# SP800-53 Baseline Security Controls for SCADA and ICS

- Development of security requirements and baseline security controls for federally owned/operated industrial/process control systems based on NIST SP800-53
- Security control mapping and gap analysis with NERC CIP standard to discover and propose modifications to remove any conflicts
- Voluntary adoption of the same or similar security requirements and baseline security controls by the private sector industrial/process control community by feeding these requirements into ISA-SP99.

# Private Sector Standards

- **Private sector standards, if widely implemented, will raise the level of control systems security**
- **Greatest chance for industry acceptance and adoption is to have security requirements published in industry standards**
  - **ISA SP99 *Industrial Automation and Control System Security* standard**
  - **IEC 62443 *Security for industrial process measurement and control –Network and system security* standard**

# The Instrumentation, Systems, and Automation Society (ISA)-SP99

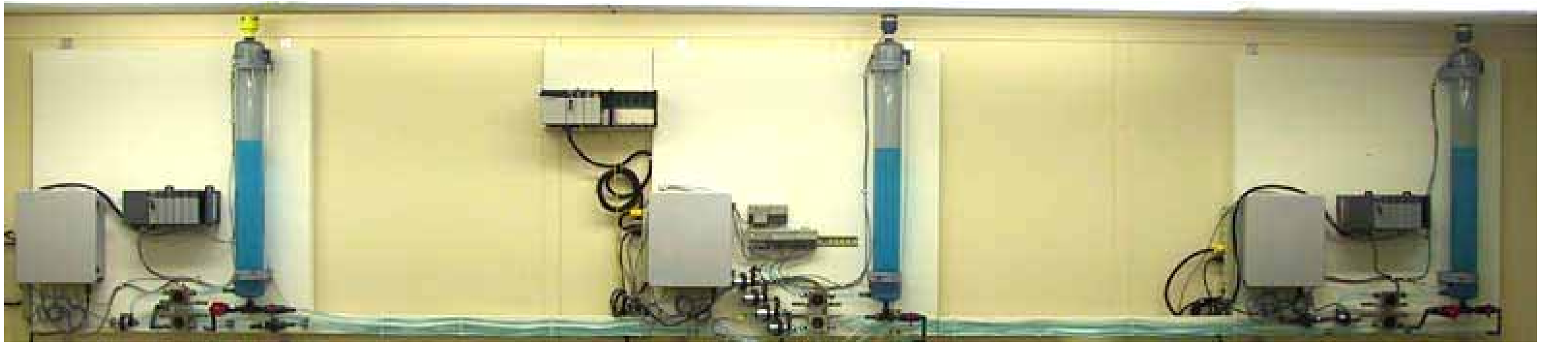
- Developing an ANSI Standard for Industrial Control System Security
  - Part 1 – Terminology, Concepts and
  - Part 2 – Establishing an Industrial Automation and Control Systems Security Program
  - Part 3 – Operating an Industrial Automation and Control Systems Security Program
  - Part 4 –Security Requirements for Industrial Automation and Control Systems

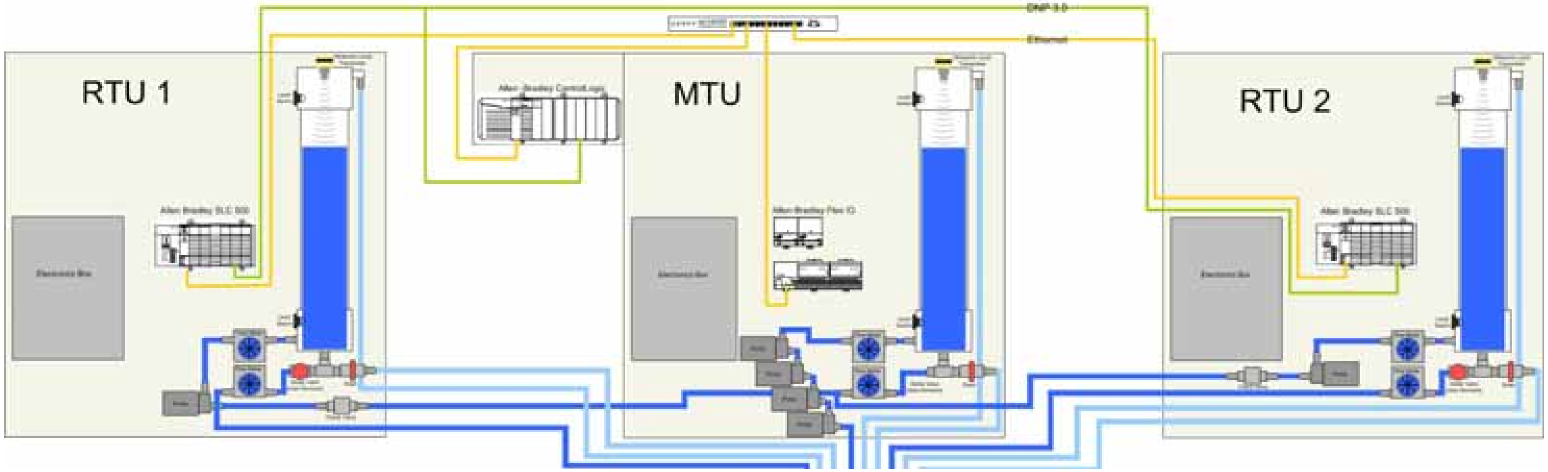
# NIST Industrial Control System Security Testbed

- Provides an industrial setting in which to
  - validate standards for process control security
  - develop performance- and conformance test methods
- Targeted outcomes:
  - development and dissemination of best practices for process control security
  - security standards for acquisition, development, and retrofit of industrial control systems

# NIST Industrial Control System Security Testbed
# Water Distribution SCADA System

- Ultrasonic Level Transmitters
- Analog Flow Meters
- DNP 3.0 Serial
- Liquid Level Switches
- Centrifugal Pumps
- Ethernet





# NIST Industrial Control System Security Testbed
# Factory Control System

- DeviceNet I/O network
- Three controller options
  - Wonderware PC-based software PLC
  - Modicon hardware PLC
  - DeltaV Hybrid Controller
- SQL database for data logging

# Antivirus Test Methods

- Develop performance tests to screen for potential problems when deploying security software in industrial control system environments
- Test procedures, and guidance with accompanying data to illustrate potential problems and solutions when deploying security software with industrial control systems
- Publication available at: http://www.isd.mel.nist.gov/projects/processcontrol/NIST_SP1058.pdf

# Contact Information

Keith Stouffer
National Institute of Standards and Technology
100 Bureau Drive
Mail Stop 8230
Gaithersburg, Maryland  20899-8230
USA

keith.stouffer@nist.gov (email)
1 301 975 3877 (phone)
1 301 990 9688 (FAX)