The NIST Cybersecurity of Industrial Control Systems Testbed

Keith A. Stouffer
Manufacturing Engineering Laboratory
National Institute of Standards and Technology

January 23, 2003

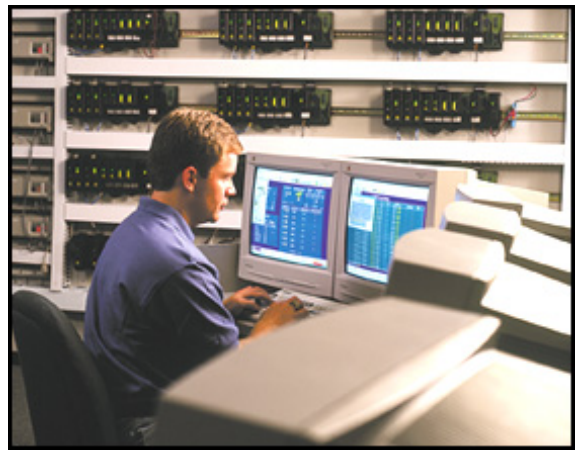
National Institute of Standards and Technology

NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.

- 3,000 employees
- 1,600 guest researchers
- $820 million annual budget
- NIST Laboratories -- National measurement standards
- Advanced Technology Program -- $640 million current R&D partnerships with industry
- Manufacturing Extension Partnership -- 400 centers nationwide to help small manufacturers
- Baldrige National Quality Award

Motivation: Critical Infrastructure Protection

- The (US) National Plan for Information Systems Protection and other reports cite industrial control systems as critical points of vulnerability in America's utilities and industrial infrastructure...



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

Risks

- Loss of Life, Endangerment of Public Health and Safety
- Social Disruption
- Loss of Production/Generation/Distribution
- Harm to Personnel and Equipment
- Environmental Damage
- Compromising of Proprietary Information
- Threat of Liability

Control System Characteristics

- Time critical
- Designed to maximize performance, reliability, flexibility, safety
- In past, typically physically isolated and based on proprietary hardware, communications
- Security has not been a significant consideration

Increased Connectivity = Increased Vulnerabilities

- Enterprise Integration
  - Across Functions and Departments
  - Across Sites/Facilities
- Remote/Web Access of Equipment and Control Information
- Open/COTS Systems
- Factory Floor Ethernet
- Strategic Partnering
- Mergers and Acquisitions
- Wireless Communications

…Which Could Be Exploited By:

- Communications or processing denial of service
- Spoofing of sensor readings or control commands
- Modification of control programs
- Interfering with safety system operation
- Changing/disabling process parameters/limits

Process Control Security Challenges

- Real time constraints - IT security technology can impact timing, inhibit performance
- Balancing of cost, 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

CIP Program Summary

- **Long-term Objective:** Integrate 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 industry to develop standards and test methods for validation and conformance

Process Control Security Requirements Forum (PCSRF)

Immediate Goal:

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 NIST and NSA work to develop the *Common Criteria for IT Security Evaluation*

Process Control Security Requirements Forum

PCSRF Representation

- EPRI (Electric Power Research Institute)
- Texaco, BP
- Georgia-Pacific
- Association of Metropolitan Water Agencies
- American Chemistry Council
- Open Group
- ISA
- National Security Agency
- Department of Energy/Sandia, PNNL
- National Center for Manufacturing Sciences (NCMS)
- Honeywell, Rockwell
- NIST (Manufacturing Engineering, Electrical and Electronics Engineering, and Information Technology Laboratories)

Requirements Development Steps

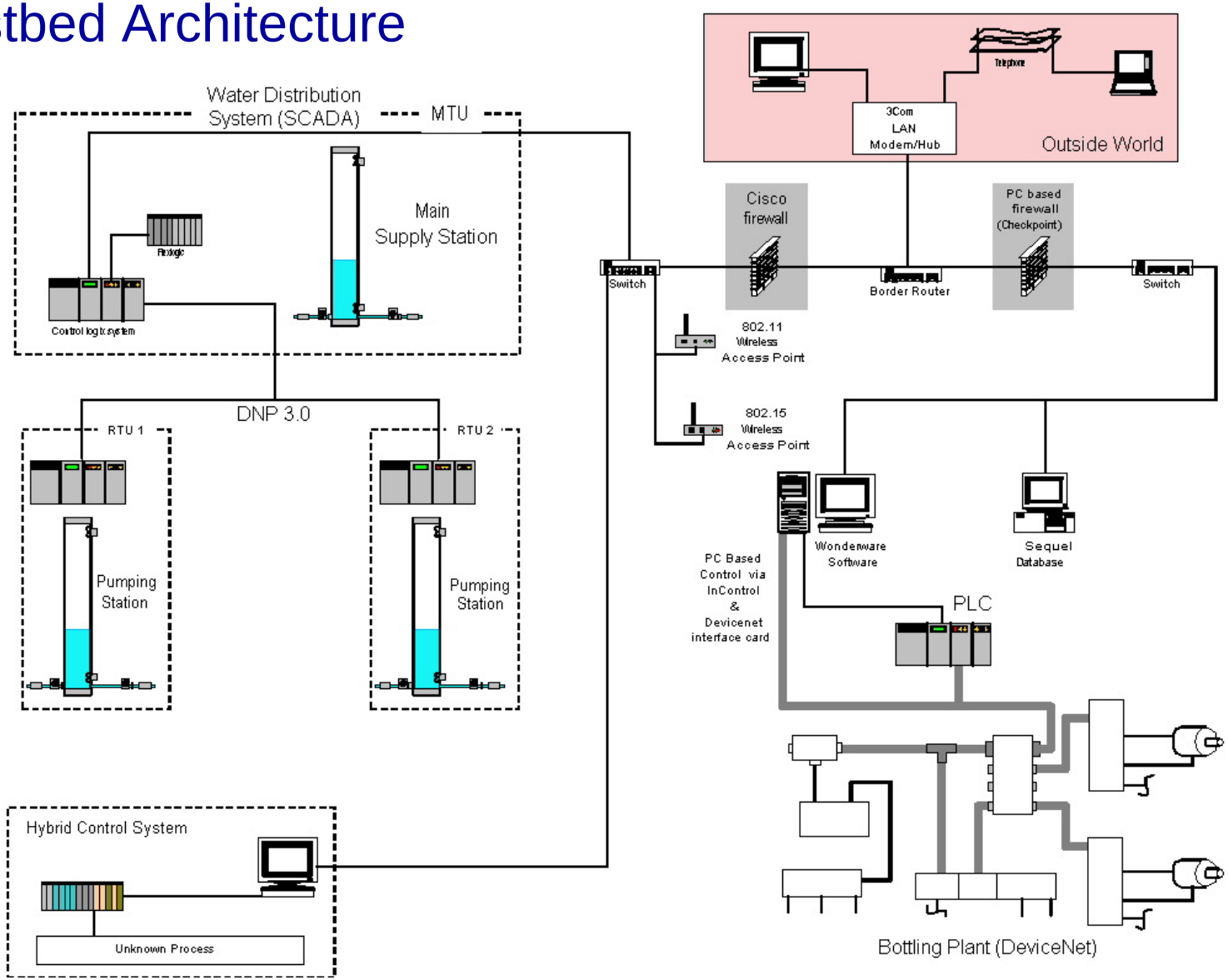
- Analyze industrial control system architectures, including analysis of threats and vulnerabilities
- Partition the system architecture for the purpose of requirements definition
- Develop information security requirements for a subset of the overall system
  - Target Definition, Security Environment, Security Objectives, Security Functional and Assurance Requirements
  - Express in procurement language accessible to process control community
- Translate information security requirements into Protection Profile(s)
- Establish testbed to develop test methods and demonstration capability

⇨ *Sector-specific workshops, cosponsored with industry organizations (NCMS, EPRI, AWWA, AGA, ACC) will be key information sources*

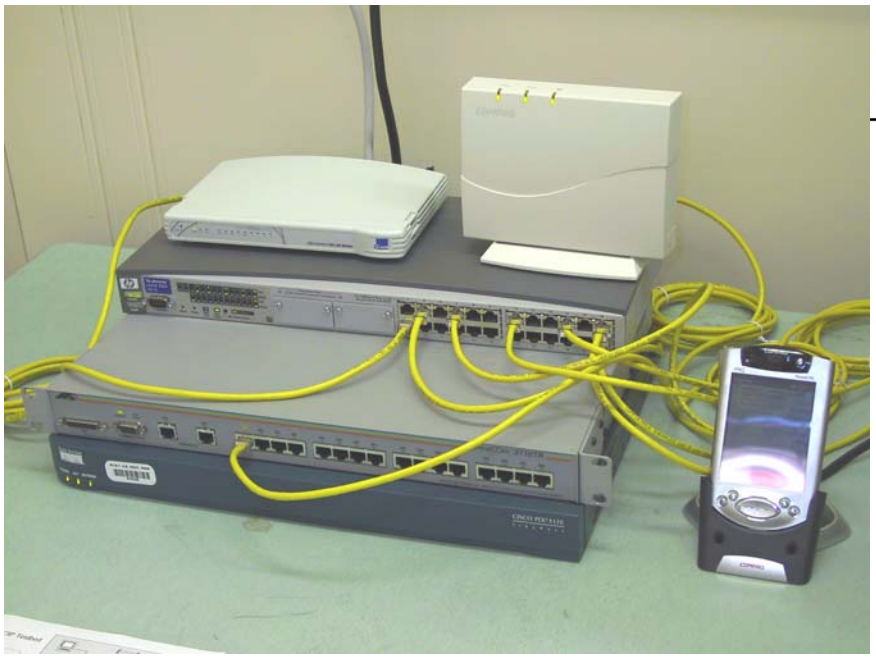
Process Control Security Testbed

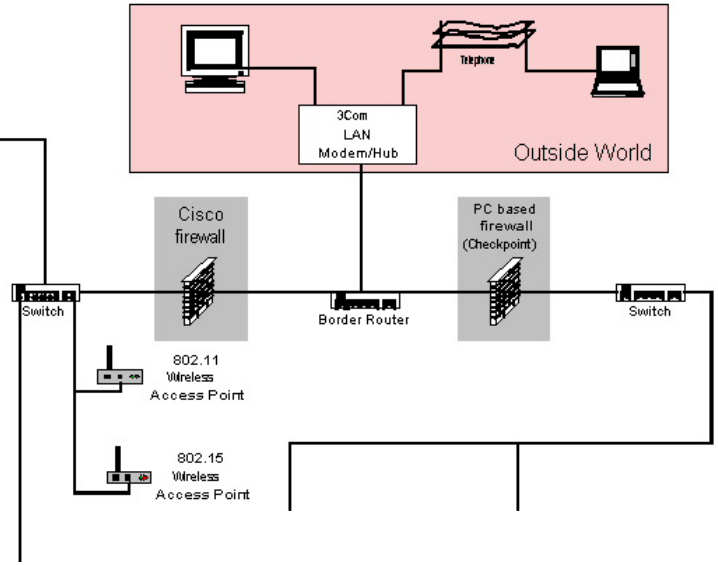
- Provides an industrial setting in which to
  - validate standards for process control security
  - develop performance- and conformance test methods
- Targeted outcomes:
  - development and dissemination of best practices for process control security
  - security standards for acquisition, development,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

Process Control Security Testbed Architecture



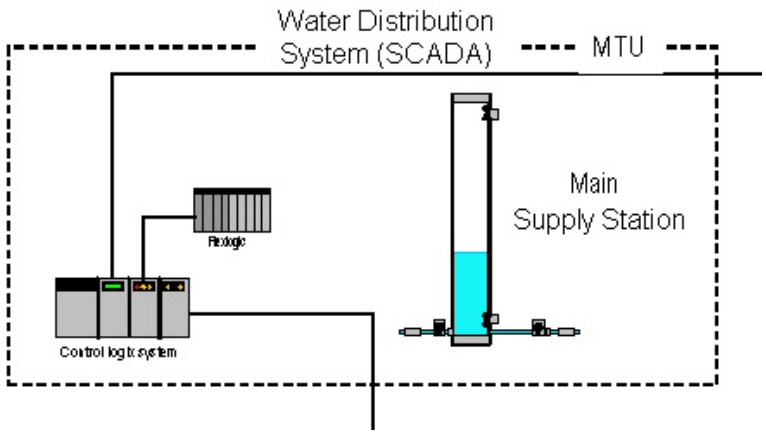
Network Hardware

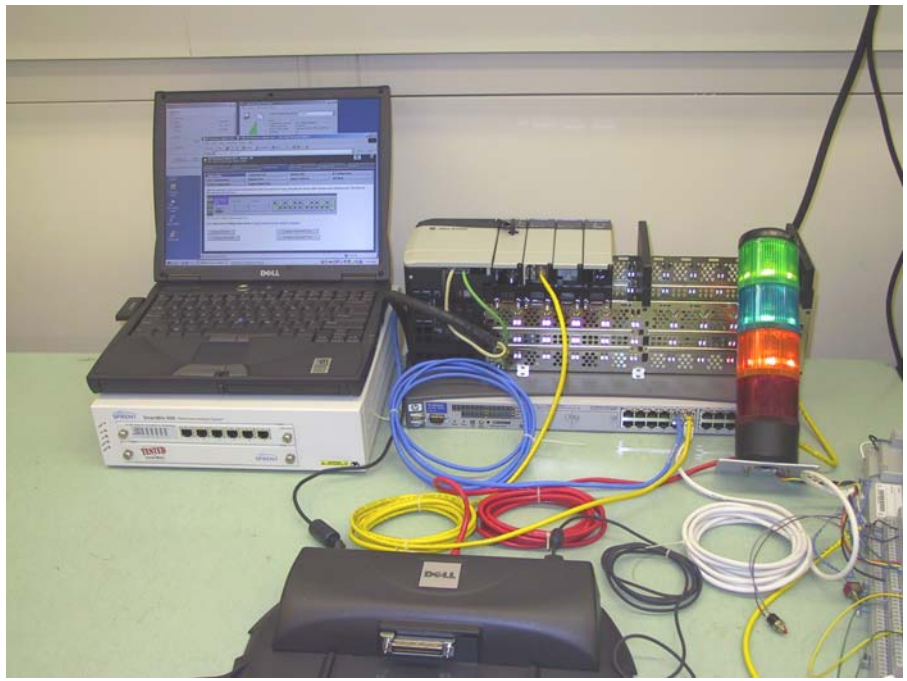




- Hardware firewall
- Ethernet switch
- Dial-up modem/4 -port hub
- 802.11a,b wireless access point
- Handheld PC

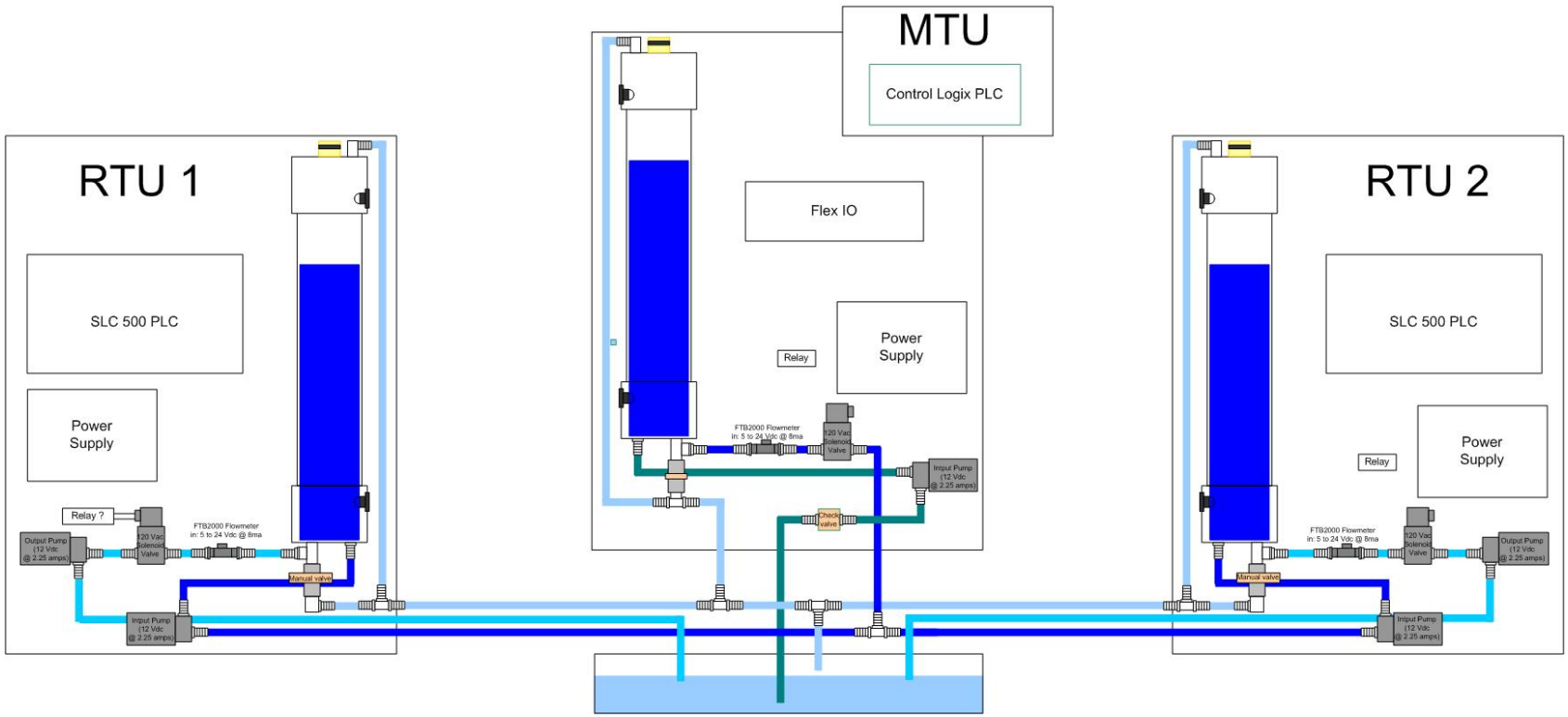
Water Distribution MTU





- Master Terminal Unit (MTU) for water distribution simulation
  - Programmable logic controller (PLC)
  - EtherNet/IP, DeviceNet and DNP 3.0 protocols

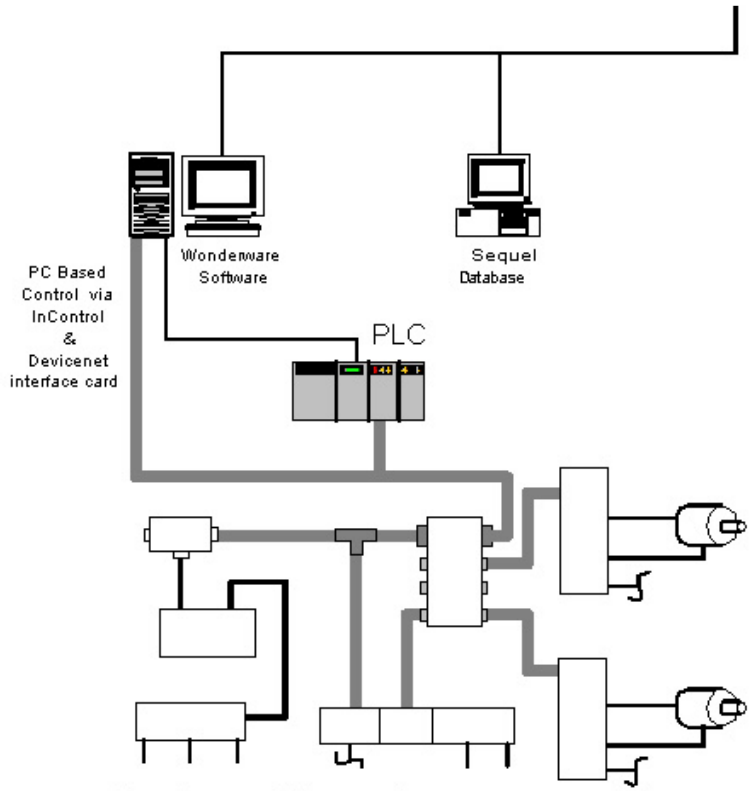
Water Distribution SCADA System



Bottling Plant PLC

- Bottling plant simulation:
  - drive motors
  - proximity switches
  - rejection actuators
  - bottle counters

- DeviceNet I/O network
- Two PLC options:
  - PC-based software
  - dedicated hardware
- SQL database for data logging



Latency and Jitter Measurement

- Effects of adding crypto-modules to existing network
- Critical parameter can be jitter of data in control loops
- How to measure with typical network traffic, crypto-modes, and communications noise
- Two protocols – Ethernet and Serial (TCP/IP and RS232)

Latency Testbed

- Three Computers used to simulate MTU, RTU and network
- Ethernet or serial communications modes

Summary

- Process control automation is heavily used in critical infrastructure
- Lack of security + increased connectivity = significant vulnerabilities; major health and safety risks
- Traditional IT security solutions don’t address real-time, embedded nature of devices and controllers
- Users and vendors are teaming to develop standards and products to address the needs
- NIST’s role is in standards validation, conformance- and performance test development

Questions?

More information:

www.isd.mel.nist.gov/projects/processcontrol
or
www.niap.nist.gov
click *Forums ⇨ Process Control*