

# NIST Industrial Control System Security Activities

Keith Stouffer  
National Institute of Standards and Technology

# NIST ICS Security Activities

NIST's role is to work with industry to develop standards, guidelines, checklist and test methods for industrial control system security

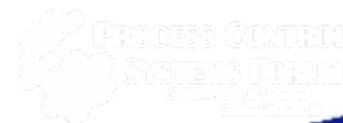
- ◆ Process Control Security Requirements Forum (PCSRF)
- ◆ SCADA Protection Profile
- ◆ SP800-82 Guide for SCADA and ICS Security
- ◆ SP800-53 Baseline Security Controls for SCADA and ICS
- ◆ Recommended Requirements for ICS Security
- ◆ Industrial Control System Security Testbed
- ◆ Support related efforts: ISA SP-99, DHS Process Control Systems Forum (PCSF), IEC 62443 (65/WG10), etc.

# 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*



# PCSRF: Over 700 registered members including:

## ICS Vendors



## Government



## IT Vendors



## Standards Organizations



ISA-SP99



ISO/IEC 15408,  
19791, 61508,  
65 (62443)



AGA 12

## End Users



Georgia-Pacific



ChevronTexaco

ExxonMobil

# PCSRF Membership

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

**On 4/25/06 There were:**

- ◆ **764 individual members from**
- ◆ **424 organizations from**
- ◆ **32 Countries (USA, Canada, Australia, Austria, Belgium, 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, Venezuela)**

# **System Protection Profile for Industrial Control Systems (SPP-ICS)**

- **151 page generic system level protection profile for ICS**
- **Presents a cohesive, cross-industry set of security requirements for new industrial process control systems based on requirements captured from numerous sector specific workshops**
- **Includes IT and non-IT security requirements**
- **Considers an entire system and addresses requirements for the entire system lifecycle**
- **A starting point for more specific system protection profiles (SCADA, DCS)**

# SCADA Protection Profile

## ◆ PCSRF Working Group

- 10 member group
- Experienced in Common Criteria, SCADA systems and requirements

## ◆ Specific functional and assurance requirements for SCADA systems

## ◆ Comprised of 2 connected PPs

- Control Center Protection Profile
- Field Device Protection Profile

## ◆ Field Device PP to be presented at the PCSRF Meeting – June 8, 2006

# Harmonization of Requirements

- ◆ **Harmonization of requirements across the Federal sector**
- ◆ **Private sector adoption (industry standards)**
- ◆ **Assessment tools that perform assessments against the standards**
- ◆ **Standard procurement language to specify the requirements in the standards**

# 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 – Workshop 4/19-20, 2006 at NIST**
- **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 communities by feeding these requirements into ISA-SP99 and IEC 65 (62443)**
- **Harmonization of requirements across Federal sector and private sector**

# 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 management, operational and technical countermeasure to mitigate the associated risks**
- ◆ **Subject Matter Expert draft released March 2006; First public draft will be released June 2006**

# Recommended Requirements document

- ◆ **DHS, the DOE National labs and NIST are creating a requirements document that can be used by all sectors in the development of control system cyber security standards, recommended practices, etc.**
- ◆ **Greatest chance for industry acceptance and adoption publish security requirements in industry standards**
- ◆ **ISA SP99 *Manufacturing 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 – Models and Terminology
  - Part 2 – Establishing a Manufacturing and Control Systems Program – NIST is the technical editor
  - Part 3 – Operating a Manufacturing and Control Systems Program
  - Part 4 – Specific Security Requirements for Manufacturing and Control Systems - Security requirements developed by NIST/ PCSRF/DOE Labs will be a starting point for Part 4 – due to start in June 2006

# Standard Procurement Language Project

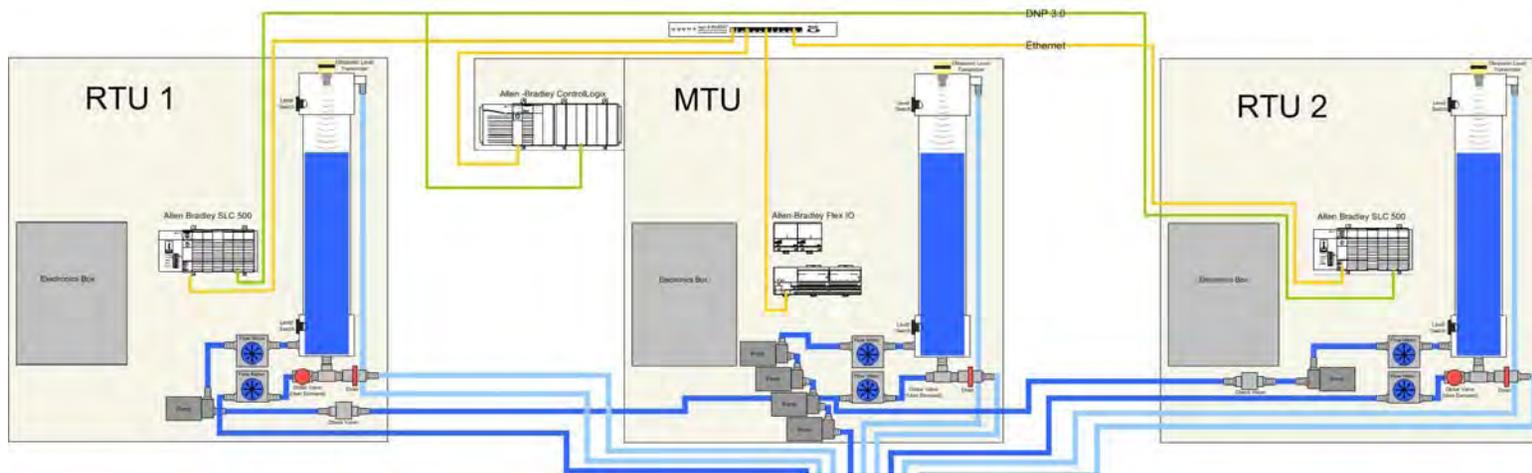
- ◆ **SANS, New York State, DHS, the DOE National labs, NIST and the private sector are currently working to develop procurement language standard so the end users have language for specifying security requirements in their contracts**

<http://www.cscic.state.ny.us/msisac/scada/>

# 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**

# Concluding thought

- ◆ ***“We must all hang together, or most assuredly we shall all hang separately” - Benjamin Franklin***

# **Additional Information**

## **PCSRF**

**<http://www.isd.mel.nist.gov/projects/processcontrol>**

## **NIST SP800-82**

**<http://csrc.nist.gov/publications/drafts.html>**

**Keith Stouffer**

**[keith.stouffer@nist.gov](mailto:keith.stouffer@nist.gov)**

**(301)975-3877**