

Setting the Standard for Automation™



NIST Industrial Control System Security Activities

EXPO 2005

Chicago, IL

Standards

Certification

Education & Training

Publishing

Conferences & Exhibits

Keith Stouffer

National Institute of Standards and Technology



- Keith is an engineer in the Intelligent Systems Division within the NIST Manufacturing Engineering Laboratory and has been at NIST for the past 15 years
- Chair of the Process Control Security Requirements Forum (PCSRF)
- Member of the Governing Board for the DHS Process Control Systems Forum (PCSF)
- Member of ISA-SP99
- US TAG member for IEC/TC 65 and IEC/SC 65C
- Bachelor's Degree in Mechanical Engineering from the University of Maryland
- Master's Degree in Computer Science from Johns Hopkins University



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

Two NIST Activities Addressing Industrial Control System Security

- Process Control Security Requirements Forum (PCSRF)
 - System Protection Profile for Industrial Control Systems
 - SCADA Protection Profile
- Special Publication SP 800-82 *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security*

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 Members



Approximately 650 registered members including:

ICS Vendors



Government



IT Vendors



Standards Organizations



ISA-SP99



ISO/IEC 15408,
19791, 61508, 65C



AGA 12

End Users



Georgia-Pacific



ChevronTexaco

ExxonMobil

On 8/31/05 There were:

- 680 individual members from
- 401 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)



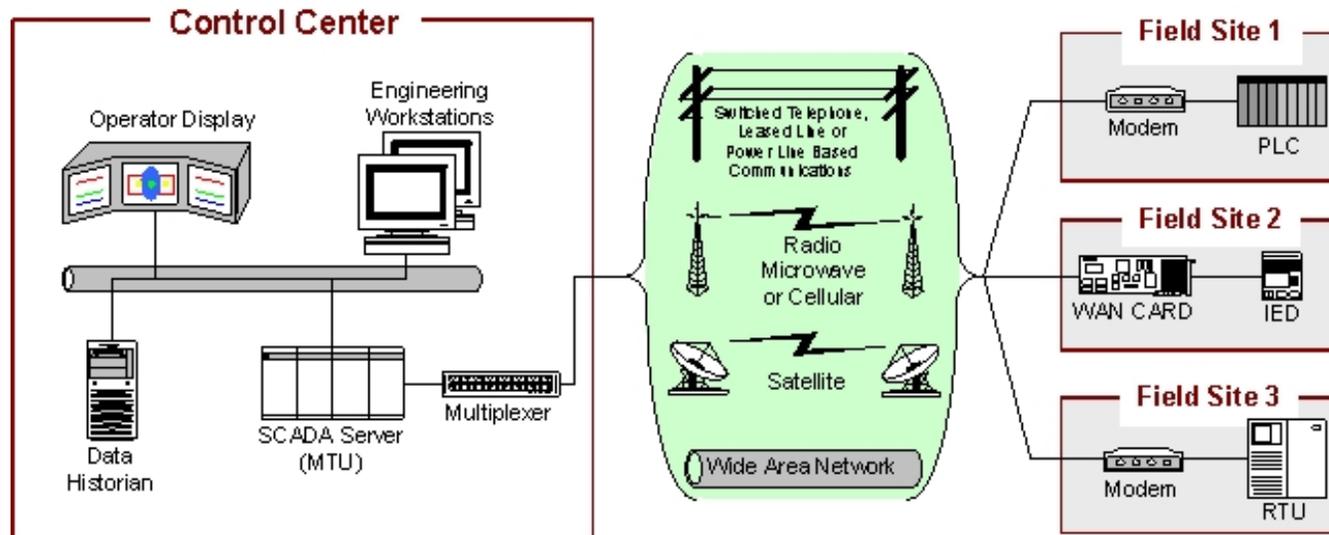
- 151 page generic system level protection profile for ICS
- Contains security functional and assurance requirements that extend ISO 15408 to address systems (ISO/IEC 19791)
- Presents a cohesive, cross-industry set of security requirements for new industrial process control systems
- Includes IT and 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)
 - A System Security Target (SST) for a specific instance of an industrial control system

- Address security throughout the system life cycle
- Defense in depth approach
- Identification and authentication - users and data
- Event recording and auditing
- Reliable and standard (consistent) time stamps
- Encryption where required
- Secure out of the box
- Policies and procedures
 - Personnel
 - Configuration and patch management

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 and Communications Protection Profile



SP 800-82 Guide to SCADA and Industrial Control System Security



- Guidance for establishing secure SCADA and Industrial Control Systems
- Provides an overview and presents typical topologies to facilitate the understanding of industrial control systems
- Identifies typical vulnerabilities, threats and consequences
- Provides guidance on security deployment including administrative, physical and technical countermeasures to mitigate the associated risks
- Final document completed by January 2006

- Executive Summary
- Introduction
- Industrial Control Systems
- Industrial Control Systems Vulnerabilities
- Industrial Control Systems Security Deployment
- Emerging Security Capabilities
- Appendices
 - Acronyms and Abbreviations
 - Glossary of Terms
 - Current Activities in SCADA/Industrial Control Security
 - Case Study

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

- Provides an overview of SCADA and industrial control systems
- Control Systems vs. Typical IT Systems
- SCADA Systems
- Industrial Process and Discrete Part Control Systems
- Control System Components and Connectivity

- Discusses SCADA and industrial control systems vulnerabilities
- Administrative Vulnerabilities (policies and procedures)
- Physical Vulnerabilities
- Platform Vulnerabilities
- Network Vulnerabilities

Industrial Control Systems Security Deployment



- Business case for security
- Layered security
- Recommended Management, Operational and Technical security controls (countermeasures) to mitigate the risk associated with the vulnerability
- Deployment model based on levels of impact from potential consequences

Security Requirements Based on Levels of Impact from Potential Consequences



- Possible model is to develop recommended security requirements based on Low, Moderate and High levels of impact from potential consequences
- Model that is used in NIST SP 800-53 *Recommended Security Controls for Federal Information Systems*

Possible Low, Moderate and High Definitions for Industrial Control Systems



- Low
 - **Product Controlled:** Non hazardous materials or products, Non-ingested consumer products
 - **Industry Examples:** Plastic Injection Molding, Warehouse Applications
 - **Security Concerns:** Protecting people, Capital investment, Ensuring uptime
- Moderate
 - **Product Controlled:** Some hazardous products and/or steps during production, High amount of proprietary information
 - **Industry Examples:** Automotive Metal Industries, Pulp & Paper, Semi-conductors
 - **Security Concerns:** Protecting people, Trade secrets, Capital investment, Ensuring uptime

Possible Low, Moderate and High Definitions for Industrial Control Systems (cont)



- High
 - **Product Controlled:** Critical Infrastructure, Hazardous Materials, Ingested Products
 - **Industry Examples:** Utilities, PetroChemical, Food & Beverage, Pharmaceutical
 - **Security Concerns:** Protecting human life, Ensuring basic social services, Protecting environment

- Risk Assessment
- Developing and Implementing a Security Program
- System and Services Acquisition
- Security Assessments

- Personnel Security
- Patch Management
- Configuration Management
- Checklists
- Network Segmentation
- Incident Response
- Disaster Recovery Planning
- Physical Protection

- User Identification, Authentication and Authorization
- Data Identification and Authentication
- Device Identification, Authentication and Authorization
- Logging
- Audit
- Secure Communications
- Access Control
- Intrusion Detection and Prevention
- Virus, Worm and Malicious Code Detection

- Discusses emerging security capabilities that are being developed in the SCADA and industrial control system sector such as device authentication for field devices and encryption modules

- Acronyms and Abbreviations
- Glossary of Terms
- Mapping of document controls to SP 800-53, ISA-SP99, ISO 17799, others?)
- Current Activities in SCADA/Industrial Control System Security
- Case study in SCADA and industrial control system security
- References

- Users, vendors and integrators are teaming to develop standards and products to address security needs
- NIST's role is to work with industry to develop standards, guidelines, checklists and test methods for industrial control system security
- More information:
- PCSRF
 - <http://www.isd.mel.nist.gov/projects/processcontrol>
- SP 800-82 (and other NIST Special Publications)
 - <http://csrc.nist.gov/publications/nistpubs/>