
*Setting the Standard for Automation™*

# Specific Security Requirements for Industrial Automation and Control Systems

## Integrating ISA-99, NIST SP 800-53, and IEC TC65 WG10 (IEC 62443)

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

# Keith Stouffer

- Mechanical Engineer in the Intelligent Systems Division within the NIST Manufacturing Engineering Laboratory – 17 years
- Project Leader of the NIST Industrial Control System Security Project
- Member of ISA-99 (WG4 and WG5)
- 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

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

# ICS Security Standards Overview

- Harmonization of ICS Standards Effort
  - Catalog of Control Systems Security:  Recommendations for Standards Developers
- US Federal ICS Standards and Guidelines
  - NIST SP800-53 ICS
  - NIST SP800-82
- Private Sector ICS Standards
  - ISA-99
  - IEC 62443

# Harmonization of ICS Standards

- Premise - Cyber security standards for control systems, 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 (e.g., ISA-99, IEC 62443)
- Standards bodies and industry associations are mainly volunteer efforts which potentially lengthen the time to develop new standards or best practices
- Many good control system security requirements exist, but are scattered among numerous industry standards, recommended practices and technical reports.

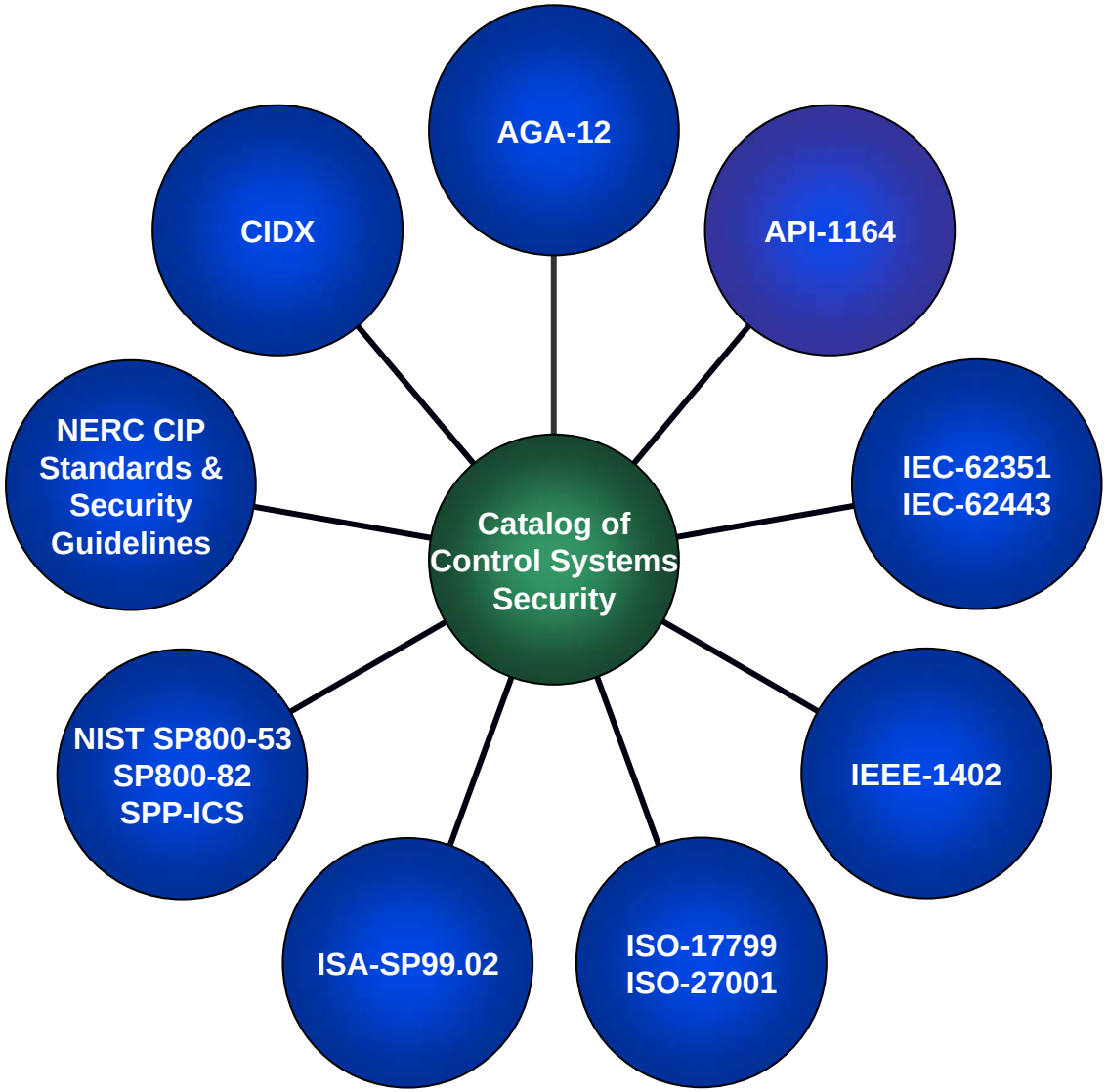
# Catalog of Control Systems Security

- A catalog of cyber security requirements document has been drafted by the DHS CSSP Standards Awareness Team that identifies requirements that can be used to facilitate the development and convergence of control system cyber security standards to be applied to the Critical Infrastructures and Key Resources (CI/KR) of United States and other nations.

# Catalog Overview

- Compilation of granular cyber security requirements written specifically for control systems
- Crosswalk that maps requirements to industry standards and technical reports
- Reference document available for use by standards bodies and industry associations to supplement or develop new cyber security standards
- Seed requirements that can be tailored to meet the needs of end users within an industry segment

# Catalog Sources



# Cross-Reference to Standards, Recommended Practices and Technical Reports

| | | | | | AGA12-1 | AGA12-2 | FIPS 140-2 | API 1164 | Security Guidelines for the Petroleum Industry | CIDX | ISO 17799 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2.1 | | Security Policy | | | | | | | | |
| 1 | | 2.1.1 | | Security Policy | X | --- | X | X | X | X | X |
| | 2.2 | | Organizational Security | | | | | | | | |
| 2 | | 2.2.1 | | Statement of Management Practice | --- | --- | --- | X | --- | X | X |
| 3 | | 2.2.2 | | Applicability | X | --- | --- | X | --- | X | X |
| 4 | | 2.2.3 | | Baseline Practices | --- | --- | --- | X | --- | X | X |
| 5 | | 2.2.4 | | Additional Control System Security Responsibility | --- | --- | --- | X | --- | X | X |
| 6 | | 2.2.5 | | Coordination of Threat Mitigation | --- | --- | --- | X | X | X | X |
| 7 | | 2.2.6 | | Security Policies for Third Parties | --- | --- | --- | X | X | X | X |

# Catalog Organization

- Grouping of requirements into families:
  - Security Policy
  - Personnel Security
  - Organizational Security
  - Physical and Environmental Security
  - Systems and Services Acquisition
  - Configuration Management
  - Risk Management and Assessment Planning
  - Systems and Communications Protection
  - Information and Document Management
  - Awareness and Training
  - Media Protection
  - Systems and Information Integrity
  - Access Control
  - Auditing and Accountability
  - Incident Response and Business Continuity
  - Monitoring and Reviewing Control System Monitoring Systems
  - Maintenance

For more information about the Catalog of Control Systems Security visit:

**www.us-cert.gov/control_systems/**

Or contact DHS CSSP at:

**cssp@dhs.gov**

# US Federal ICS Standards and Guidelines

## NIST Industrial Control System (ICS) Security Project

- Joint MEL/ITL project, in collaboration with federal and industry stakeholders, to develop standards, guidelines and test methods to help secure these critical control systems in harmony with their demanding safety and reliability requirements.

http://csrc.nist.gov/sec-cert/ics

# The Risk Management Framework

***Starting Point***

**FIPS 199 / SP 800-60**

**Security Categorization**

Define criticality /sensitivity of information system according to potential impact of loss

**FIPS 200 / SP 800-53**

**Security Control Selection**

Select minimum (baseline) security controls to protect the information system; apply tailoring guidance as appropriate

**FIPS 200 / SP 800-53 / SP 800-30**

**Security Control Refinement**

Use risk assessment results to supplement the tailored security control baseline as needed to ensure adequate security and due diligence

**SP 800-18**

**Security Control Documentation**

Document in the security plan, the security requirements for the information system and the security controls planned or in place

**SP 800-70**

**Security Control Implementation**

Implement security controls; apply security configuration settings

**SP 800-53A**

**Security Control Assessment**

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements)

**SP 800-37**

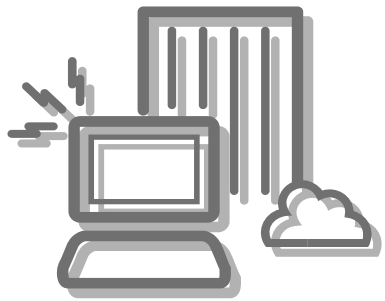
**System Authorization**

Determine risk to agency operations, agency assets, or individuals and, if acceptable, authorize information system operation

**SP 800-37 / SP 8800-53A**

**Security Control Monitoring**

Continuously track changes to the information system that may affect security controls and reassess control effectiveness



# US Federal ICS Security Standards and Guidelines Strategy

- Add control systems domain expertise to:
  - Already available IT security Risk Management Framework
  - Provide workable, practical solutions for control systems – without causing more harm than the incidents we are working to prevent

- This expertise takes the form of specific cautions, recommendations & requirements for application to control systems - throughout both technologies and programs
  - ICS Augmentation of NIST SP 800-53 *Recommended Security Controls for Federal Information Systems*
  - NIST Special Publication (SP) 800-82 *Guide to Industrial Control System (ICS) Security*

# The Risk Management Framework

*Starting Point*

**FIPS 199 / SP 800-60**

**Security Categorization**

Define criticality /sensitivity of information system according to potential impact of loss

**FIPS 200 / SP 800-53**

**Security Control Selection**

Select minimum (baseline) security controls to protect the information system; apply tailoring guidance as appropriate

**FIPS 200 / SP 800-53 / SP 800-30**

**Security Control Refinement**

Use risk assessment results to supplement the tailored security control baseline as needed to ensure adequate security and due diligence

**SP 800-18**

**Security Control Documentation**

Document in the security plan, the security requirements for the information system and the security controls planned or in place

**SP 800-70**

**Security Control Implementation**

Implement security controls; apply security configuration settings

**SP 800-53A**

**Security Control Assessment**

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements)

**SP 800-37**

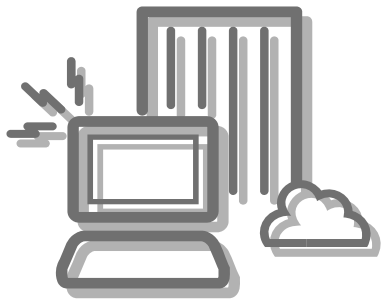
**System Authorization**

Determine risk to agency operations, agency assets, or individuals and, if acceptable, authorize information system operation

**SP 800-37 / SP 8800-53A**

**Security Control Monitoring**

Continuously track changes to the information system that may affect security controls and reassess control effectiveness



# NIST SP 800-53

- NIST SP 800-53 *Recommended Security Controls for Federal Information Systems*, which was developed for traditional IT systems, contains mandatory information security requirements for all non-national security information and information systems that are owned, operated, or controlled by federal agencies.

- NIST SP 800-53 provides the security controls that need to be applied to secure the system. It does not specify how the controls need to be implemented.

# NIST SP 800-53 Structure

17 Control Families
171 Controls (Requirements)

- Access Control
- Awareness and Training
- Audit and Accountability
- Certification, Accreditation, and Security Assessments
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental
- Planning
- Personnel Security
- Risk Assessment
- Systems and Services Acquisition
- System and Communications Protection
- System and Information

# NIST SP 800-53 Control Example

**AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING**

Control: The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

Supplemental Guidance: Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

Control Enhancements:

**(1) The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.**

**(2) The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment: organization-defined list of inappropriate or unusual activities that are to result in alerts*].**

| | | |
|---|---|---|
| **LOW** Not Selected | **MOD** AU-6 (2) | **HIGH** AU-6 (1) (2) |

# Augmenting NIST SP 800-53 for ICS

- NIST SP 800-53 contains mandatory information security requirements for all non-national security information and information systems that are owned, operated, or controlled by federal agencies. ICS are information systems.
- When organizations attempted to utilize SP 800-53 to protect ICS, it led to difficulties in implementing SP 800-53 counter-measures because of ICS-unique needs

# Changes made to NIST SP 800-53

- Original NIST SP 800-53 controls were not changed
- Additional guidance was added to address ICS
  - ICS Supplemental Guidance
  - ICS Enhancement Supplemental Guidance
- Additional guidance provides information on how the control applies in ICS environments, or provides information as to why the control may not be applicable in ICS environments.
- Additional guidance was added to 68 of 171 controls
  - ICS Supplemental Guidance added to 59 controls
  - ICS Enhancement Supplemental Guidance added to 22 controls

# Example ICS Supplemental Guidance

## CA-2 SECURITY ASSESSMENTS

**ICS Supplemental Guidance:**

The assessor fully understands the corporate cyber and ICS security policies and procedures and the specific health, safety, and environmental risks associated with a particular facility and/or process. A production ICS may need to be taken off-line, or replicated to the extent feasible, before the assessments can be conducted. If a ICS must be taken off-line for assessments, assessments are scheduled to occur during planned ICS outages whenever possible.

# NIST SP 800-53 ICS

- Draft NIST SP 800-53 ICS is a security standard that addresses both general IT systems as well as ICS. This allows the federal agencies, as well as the private sector if desired, to use one document to determine the proper security controls for their IT systems as well as to effectively secure their industrial control systems while addressing their unique requirements.

- Draft NIST SP 800-53 ICS:
  - Clean Version
    - http://csrc.nist.gov/sec-cert/ics/papers/ICS-Augmentation-Appx-F-800-53-rev1_clean_22jun07.pdf
  - Markup Version
    - http://csrc.nist.gov/sec-cert/ics/papers/ICS-Augmentation-Appx-F-800-53-rev1_blueline_22jun07.pdf

# NIST SP 800-53 Security Baselines

- LOW Baseline - Selection of a subset of security controls from the master catalog consisting of ***basic*** level controls
- MOD Baseline - Builds on LOW baseline. Selection of a subset of controls from the master catalog—***basic*** level controls, additional controls, and control ***enhancements***
- HIGH Baseline - Builds on MOD baseline. Selection of a subset of controls from the master catalog—***basic*** level controls, additional controls, and control ***enhancements***

- ***How do we categorize ICS?***

# Low Impact System

# Possible ICS Impact Level Definitions

- **Low Impact**
  - **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 Impact Systems

# Possible ICS Impact Level Definitions

- **Moderate Impact**
  - **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

# High Impact System

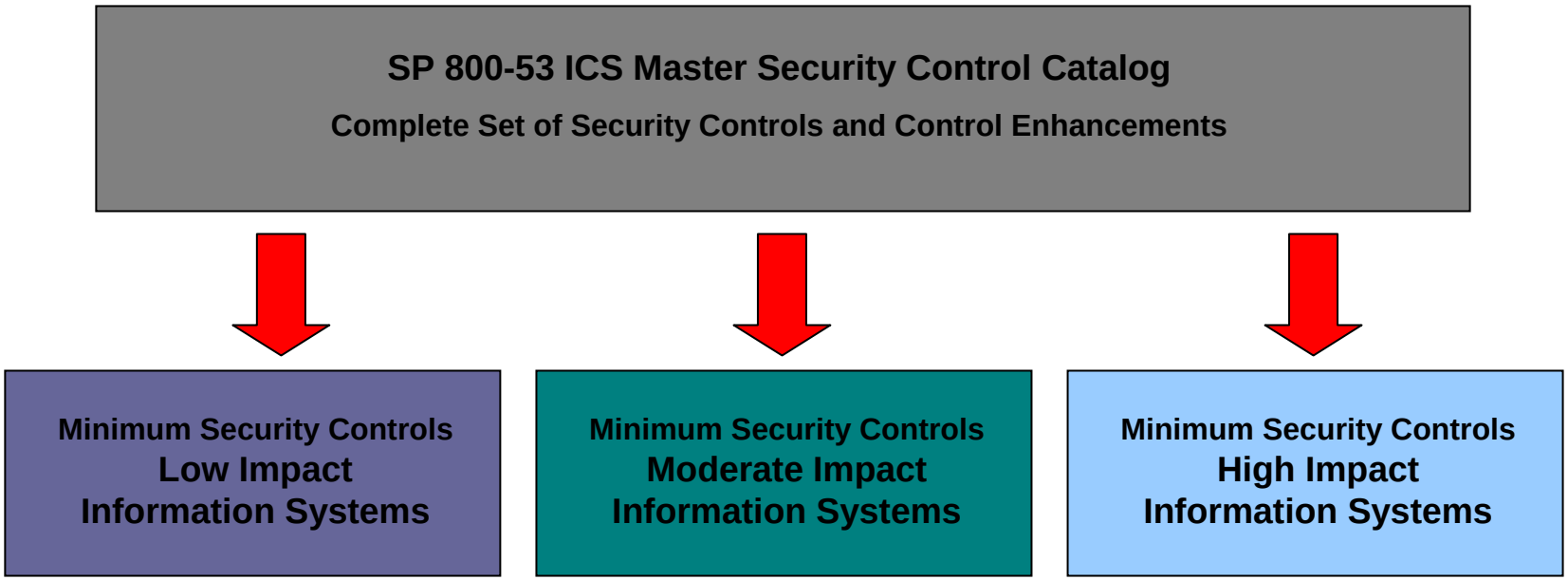

# High Impact System !!!

# Possible ICS Impact Level Definitions

- **High Impact**
  - **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

# More High Impact Systems ☺

# Security Control Baselines




***Baseline #1***

Selection of a subset of security controls from the master catalog—consisting of ***basic*** level controls

***Baseline #2***

Builds on low baseline. Selection of a subset of controls from the master catalog—***basic*** level controls, additional controls, and control ***enhancements***

***Baseline #3***

Builds on moderate baseline. Selection of a subset of controls from the master catalog—***basic*** level controls, additional controls, and control ***enhancements***

# Minimum Security Controls

- Minimum security controls, or baseline controls, defined for low-impact, moderate-impact, and high-impact information systems—
  - Provide a ***starting point*** for organizations in their security control selection process
  - Are used in conjunction with ***tailoring guidance*** that allows the baseline controls to be adjusted for specific operational environments
  - Support the organization's ***risk management process***

# NIST SP 800-82

- Guide to Industrial Control Systems Security
  - Provide guidance for establishing secure SCADA and ICS, including implementation guidance for SP 800-53 ICS controls
- Content
  - Overview of  ICS
  - ICS Characteristics, Threats and Vulnerabilities
  - ICS Security Program Development and Deployment
  - Network Architecture
  - ICS Security Controls
  - Appendixes
    - Current Activities in Industrial Control Systems Security
    - Emerging Security Capabilities
    - ICS in the FISMA Paradigm

# NIST SP 800-82

- Initial public draft released September 2006 - public comment period through December 2006.
  - http://csrc.nist.gov/publications/drafts.html
  - Downloaded over 250,000 times

- Second public draft released September 2007 – public comment period until November 30, 2007.

# Private Sector ICS Standards

- Your standards!
- Scope includes
  - SCADA/EMS
  - DCS
  - PLCs
  - RTUs/IEDs
  - Transmitters, meters, control valves, HMIs, …
  - Enterprise applications, to the extent they can affect control

# ISA-99

- Chairman:  Bryan Singer
- Developing an ANSI Standard for Industrial Automation and Control System Security
  - Part 1 – Models and Terminology
  - Part 2 – Establishing an Industrial Automation and Control Systems Program

    Part 3 – Operating an Industrial Automation and Control Systems Program
  - Part 4 – Technical Security Requirements for Industrial Automation and Control Systems

  - Catalog of Control Systems Security and NIST SP800-53 ICS have been provided to ISA-99 as references to consider in the development of the standard

http://www.isa.org/MSTemplate.cfm?MicrosoftID=988&CommitteeID=6821

# ISA-99 - Part 4

- Designation:
  - ANSI/ISA-d99.00.04
- Topic:
  - Specific Technical Security Requirements for Industrial Automation and Control Systems
- Leaders:
  - Johan Nye, Tom Phinney: Co-chairs
  - Dennis Holstein:  Editor

# ISA-99 needs participation

- Involvement
  - Contribute material to the standards or technical reports
  - Commit time to review and comment
  - Collaborate across industries and organizations
- Promotion and Advocacy
  - Affirm the need for standards and guidance
  - Promote new and improved technology

# How to participate in ISA-99

- Do you have something to add?
- ISA-99 Meeting: Thursday, October 4, 2007 – Reliant Center:  8:00 AM – 10:00 AM
- This is a great opportunity to learn about the committee and to get involved!

- Send email to:
  - Bryan Singer, bsinger74@gmail.com, Committee Chairman
  - Charley Robinson, crobinson@isa.org, ISA Standards
  - Provide your contact information and area of expertise or interest.

# IEC TC65/WG10 and IEC 62443

- Convenor: Tom Phinney (US)
- Approved work item proposal: 65/360/NP
- Object: Create a three-part standard

  "IEC 62443, *Security for industrial process measurement and control – Network and system security*"
- Scope: Establish requirements for securing access to industrial process measurement and control networks and devices on those networks

# IEC 62443

- IEC 62443 *Security for industrial process measurement and control –Network and system security* standard
  - 62443-1, *Framework and threat-risk analysis*
  - 62443-2, *Security assurance:  principles, policy and practice*
  - 62443-3, *Sets of security requirements for security elements in typical scenarios*

  - Catalog of Control Systems Security and NIST SP800-53 ICS have been provided to IEC TC65/WG10 as references to consider in the development of the standard

http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=e&wwwprog=dirwg.p&progdb=db1&ctnum=2931

# IEC 62443 status and plans

- Decision made to take draft material for eventual IEC 62443-3 to ISA-99/WG4, for joint development as a dual-labeled ISA standard and IEC technical specification
  - IEC TC65/WG10 contributors are already ISA-99 members
  - Work on this document will be in ISA-99/WG4
  - Work on IEC 62443-1 and -2 will continue in IEC TC65/WG10
  - Maintenance of joint ISA/IEC document will be in ISA; the others will be in IEC
  - Joint development as IEC 62443-3 pre-resolves conflict that would otherwise arise when ISA 99.04 would be brought to IEC TC65/WG10 for promulgation as an international standard

# NIST ICS Security Project Contact Information

***Project Leaders***


**Keith Stouffer**
**(301) 975-3877**
**keith.stouffer@nist.gov**

**Dr. Stu Katzke**
**(301) 975-4768**
**skatzke@nist.gov**

**sec-ics@nist.gov**


***Web Pages***

**Federal Information Security Management Act (FISMA) Implementation Project**

**http://csrc.nist.gov/sec-cert**

**NIST ICS Security Project**

**http://csrc.nist.gov/sec-cert/ics**

# Thank You Very Much!