Industrial Control System Security

NIST Industrial Control System
Cyber Security Workshop
23 October 2009

Presentation Topics

- Threats, risks, tactical initiatives
- Industrial Control System (ICS) Overview
- Federal ICS Security Standards and Guidelines
  - NIST SP800-53, Revision 3

The Threat Situation

Continuing serious cyber attacks on federal information systems, large and small; targeting key federal operations and assets…

- Attacks are organized, disciplined, aggressive, and well resourced; many are extremely sophisticated.
- Adversaries are nation states, terrorist groups, criminals, hackers, and individuals or groups with intentions of compromising federal information systems.
- Significant exfiltration of critical and sensitive information and implantation of malicious software.
- Errors and omissions remain a significant concern.

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
- **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

Case Study

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

Sewerage System Attack in Maroochy Shire, Queensland, Australia

- Disgruntled former employee of contractor decided to get even
- On at least 46 occasions issued radio commands to the sewage equipment
  - **Caused 800,000 liters of raw sewage to spill out into local parks, rivers and even the grounds of a Hyatt Regency hotel**
  - **Marine life died, the creek water turned black and the stench was unbearable for residents**

Case Study

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

Rapid Transit Collision

- **Event**: Train control system failed to detect stationary train (June 22, 2009)
- **Industry**: Rapid Transit
- **Location**: Washington DC Metro
- **Impact**:
  - Nine deaths

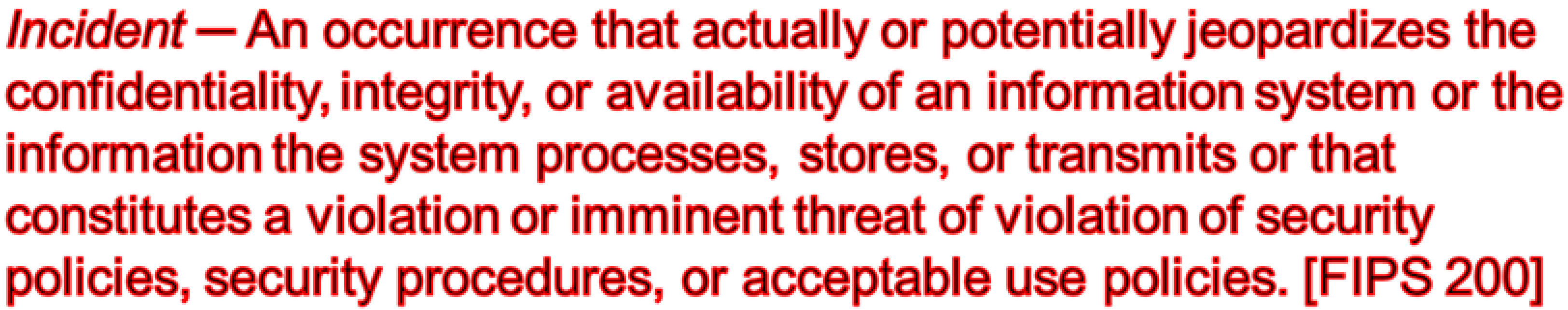
- **Lessons learned**:
  - Signal system designed to prevent crashes inadequate
  - Independent safety system necessary, such as San Francisco's BART

More Information

http://www.washingtonpost.com/wp-dyn/content/article/2009/09/22/AR2009092204280.html

(or more recent – ongoing investigation)

Observation: Difficult to Determine What's Happening



Incident — An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. [FIPS 200]

- Response must be timely
- Differences for malicious and non-malicious incidents are secondary
  - **Generally ICS systems lack adequate forensic mechanisms**
  - Difficult to differentiate attacks from malfunctions
  - Determining cause of ICS malfunction may require extensive analysis.
  - When/why is it important to determine whether intentional attack, or unintentional flaw or error?
  - Difficult to protect against insider attacks

Examples: Difficult to Determine What's Happening

- National Transportation Safety Board (NTSB) advising rail and rapid transit operators to examine train control systems ─ before investigation of June 22, 2009 METRO accident is complete
- In the Maroochy wastewater hack, the sewage discharge valve was hacked 20 times before it was recognized that it was a malicious attack and not just mechanical or electrical problems
- Cause of Bellingham gasoline spill and fire will never be known because
  - Inadequate audit and log retention
  - Operators invoked Fifth Amendment

What is at Risk?

- Federal information systems supporting Defense, Civil, and Intelligence agencies within the federal government.
- Private sector information systems supporting U.S. industry and businesses (intellectual capital).
- Information systems supporting critical infrastructures within the United States (public and private sector) including:
  - Energy (electrical, nuclear, gas and oil, dams)
  - Transportation (air, road, rail, port, waterways)
  - Public Health Systems / Emergency Services
  - Information and Telecommunications
  - Defense Industry
  - Banking and Finance
  - Postal and Shipping
  - Agriculture / Food / Water / Chemical

NIST Tactical Initiatives

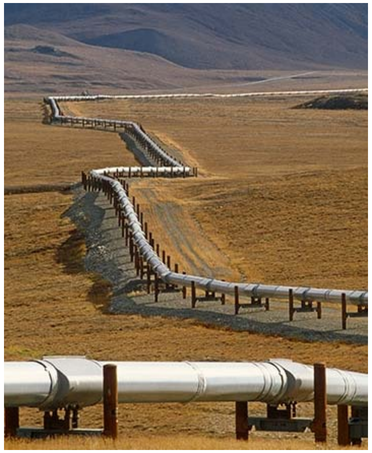
- Update security controls catalog and baselines
  - **Delivery vehicle: NIST Special Publication 800-53, Revision 3**
  - *Joint Task Force Transformation Initiative* Interagency Working Group with representatives from the Civil, Defense, and Intelligence Communities
- Develop enterprise-wide risk management guidance
  - **Delivery vehicle: NIST Special Publication 800-39**
- Restructure the current certification and accreditation process for information systems
  - **Delivery vehicle: NIST Special Publication 800-37, Revision 1**

Industrial Control Systems (ICS) Overview

- **Industrial Control System (ICS)** is a general term that encompasses several types of control systems including:
  - Supervisory Control and Data Acquisition (SCADA) systems
  - Distributed Control Systems (DCS)
  - Other control system configurations such as skid-mounted Programmable Logic Controllers (PLC)
- ICS are specialized Information Systems that physically interact with the environment
- Many ICS are components of the Critical Infrastructure
- They are moving from isolated analog systems to interconnected digital systems
  - Using Internet Protocols (IP)
  - Resembling IT network systems

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

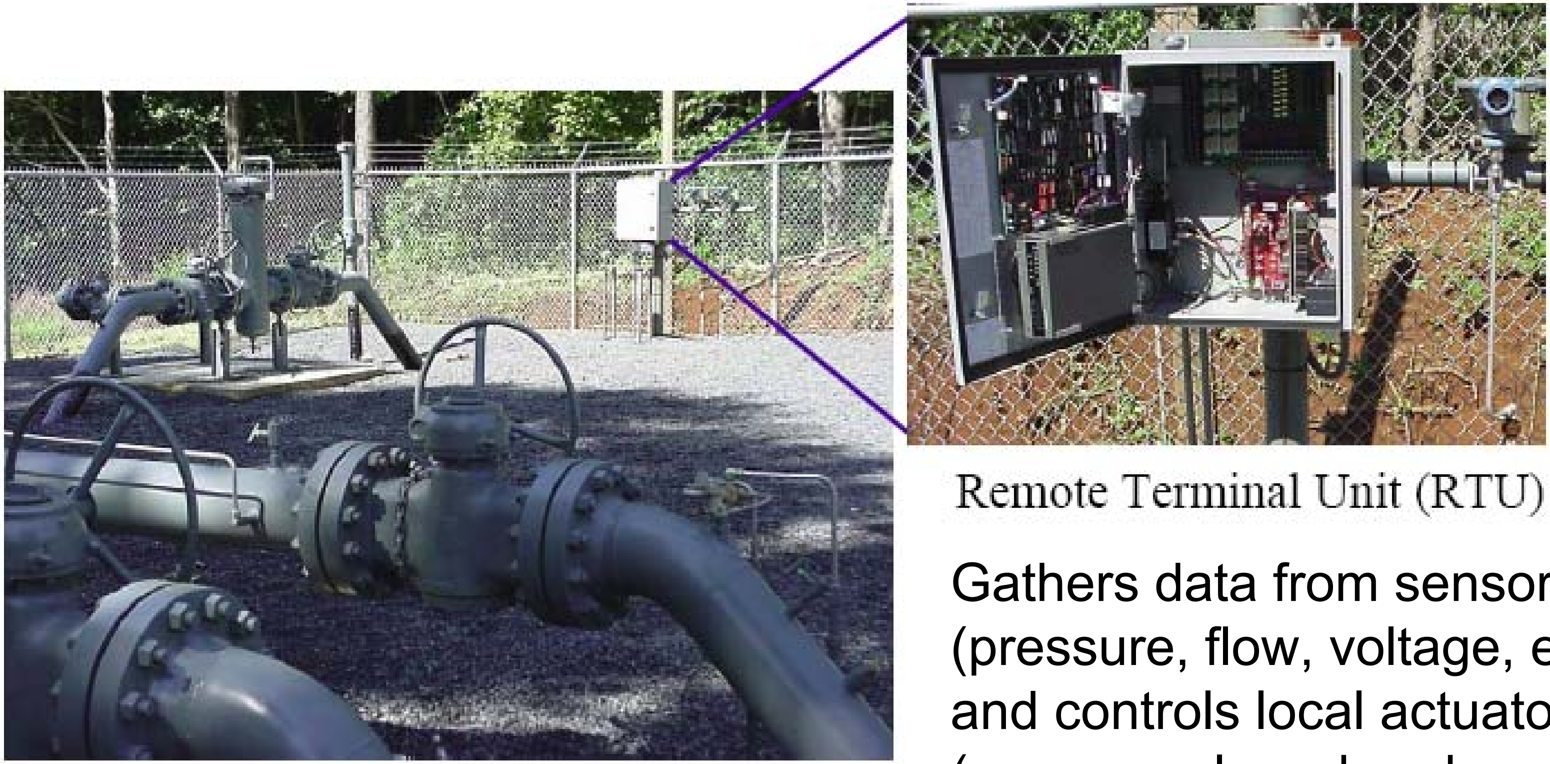
Provides control of circuit breakers, switches, etc.

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.)

DCS Examples

Electric Power Generation

Manufacturing

Refineries

Significant Potential Impact of Security Incident

- Possible major disruption of services or loss of control
  - ‘Accidental’ malware can slow entire ICS due to excessive communications load
  - Remediation can be slow despite best efforts
- Disruption can cause substantial economic loss

- Can interfere with logistical mission support
  - “…the way to delay American response is to crack the logistics systems”

[1] *Description of Limitation and Potential Mitigation Strategies for Ensuring NAS Continuity of Operations: Provisional Findings*, Carrigan, et al., Figure 3-2, WN 04W20, July 2004, The MITRE Corporation, McLean, VA

[2] *Economic Values for FAA Investment and Regulatory Decisions, A Guide, Draft Final Report*, December 31, 2004, Contract No. DTFA 01-02-C00200, GRA, Incorporated

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-Real-time	Real-time
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 Technology Characteristics

Information Technology	Industrial Control
Mostly COTS	Considerably application specific
Technology refresh ~ 5 years	Technology refresh ~ 20 years ▪ Resource and bandwidth constrained
Range of size and complexity	Often large and complex system-of-systems
Frequent patching supported	Patching difficult ▪ Resources often not available ▪ ICS software incompatibilities

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, environmental damage
Recover by reboot	Fault tolerance essential

These differences create huge differences in acceptable security practice

U.S. Federal ICS Security 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.

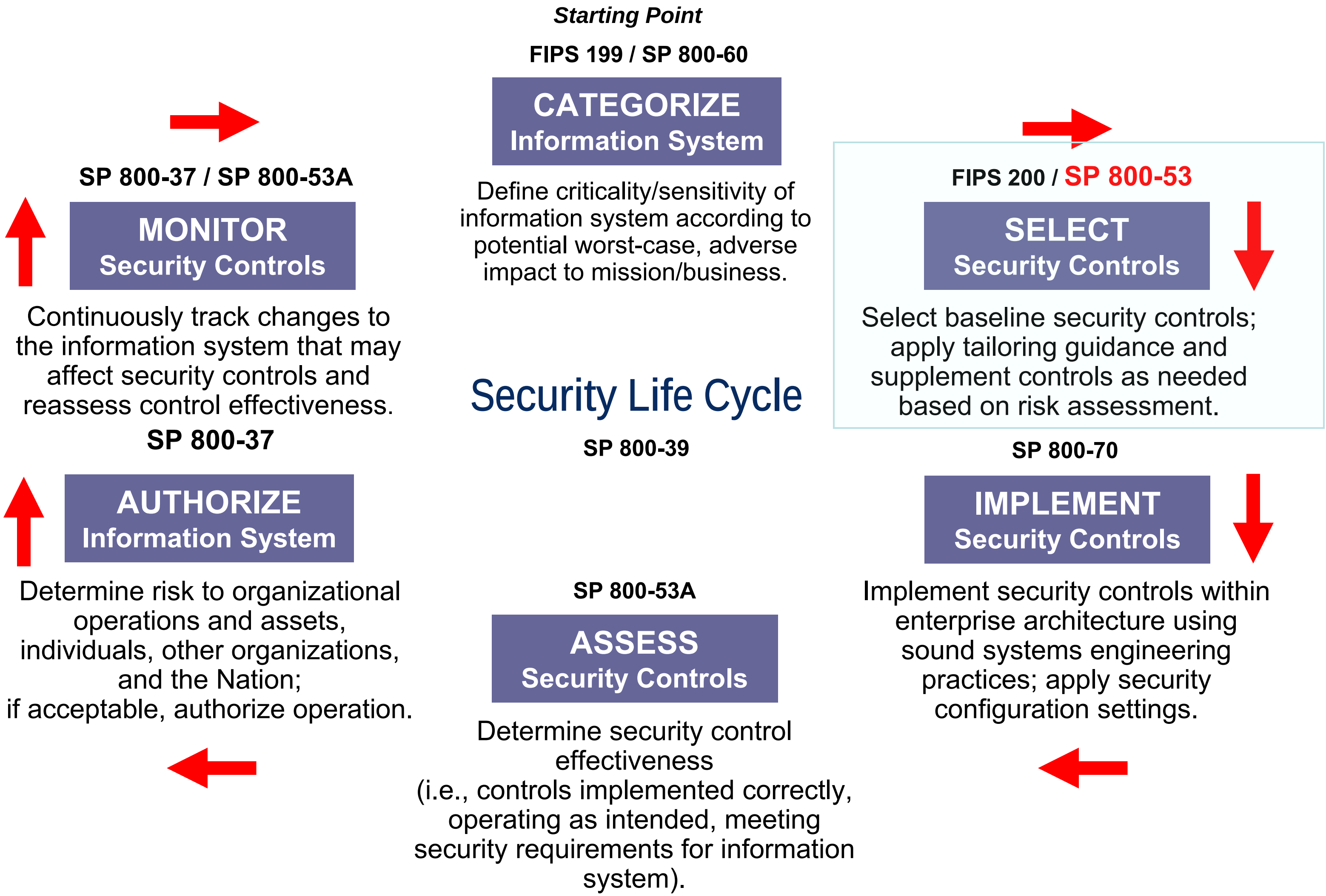
http://csrc.nist.gov/sec-cert/ics

U.S. Federal ICS Security Standards and Guidelines Strategy

- Integrate control systems domain expertise with 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 SP 800-82 *Guide to Industrial Control System (ICS) Security*

NIST Risk Management Framework



Starting Point

FIPS 199 / SP 800-60

CATEGORIZE
Information System

Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

FIPS 200 / SP 800-53

SELECT
Security Controls

Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

SP 800-70

IMPLEMENT
Security Controls

Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

SP 800-53A

ASSESS
Security Controls

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

SP 800-37

AUTHORIZE
Information System

Determine risk to organizational operations and assets, individuals, other organizations, and the Nation;
if acceptable, authorize operation.

SP 800-37 / SP 800-53A

MONITOR
Security Controls

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

Security Life Cycle

SP 800-39

NIST SP 800-53 *Recommended Security Controls for Federal Information Systems*

- Developed for traditional IT systems
  - Revision 3 developed by the *Joint Task Force Transformation Initiative Interagency Working Group with representatives from the Civil, Defense, and Intelligence Communities* ‡
  - Security control catalog incorporates best practices in information security from the United States Department of Defense, Intelligence Community, and Civil agencies
  - Standardized set of management, operational, and technical controls that provide a common specification language for information security of both national security and non national security information
  - Does not specify how the controls are to be implemented
- Control selection process based on risk assessment
  - Select initial set of baseline security controls
  - Tailoring baseline security controls
  - Supplement tailored baseline.

‡Changes is rev 3 indicated in this font and color

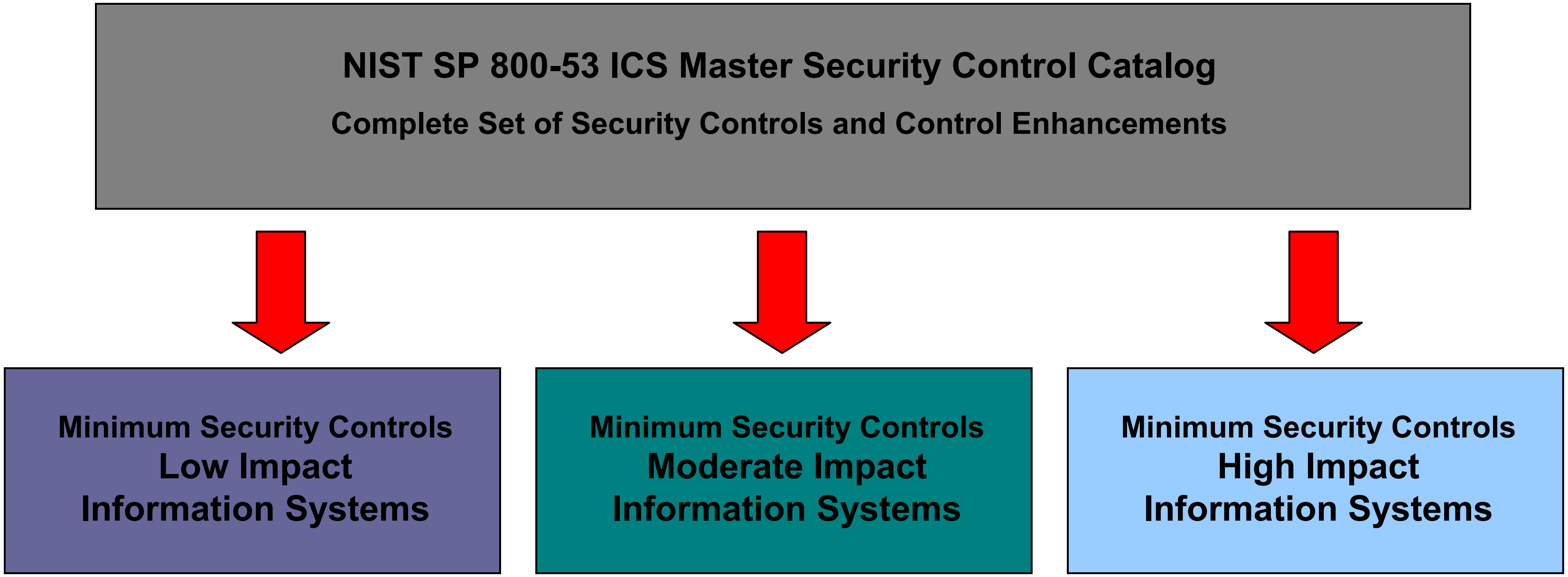
NIST SP 800-53 Control Families

IDENTIFIER	FAMILY
AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
CA	Security Assessment and Authorization
CM	Configuration Management
CP	Contingency Planning
IA	Identification and Authentication
IR	Incident Response
MA	Maintenance
MP	Media Protection
PE	Physical and Environmental Protection
PL	Planning
PS	Personnel Security
RA	Risk Assessment
SA	System and Services Acquisition
SC	System and Communications Protection
SI	System and Information Integrity
PM	Program Management

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***
- Categorization based on the potential level of impact if the **Availability, Integrity or Confidentiality** of the system or information on the system is compromised.
- ***How do we categorize ICS?***

Security Control Baselines



NIST SP 800-53 ICS Master Security Control Catalog

Complete Set of Security Controls and Control Enhancements

Minimum Security Controls
Low Impact
Information Systems

Minimum Security Controls
Moderate Impact
Information Systems

Minimum Security Controls
High Impact
Information Systems

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***

Augmenting NIST SP 800-53 to address ICS

- 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 characteristics.
- NIST held 2 Workshops (April 2006 and March 2007) with stakeholders to discuss issues and develop ICS material for SP 800-53. 2 drafts were released for public vetting before SP 800-53, Rev 2 was finalized December 2007.
- New controls and baseline additions in rev 3 based on experience

Additions made to NIST SP 800-53 for ICS

- Original NIST SP 800-53 controls were not changed
- Additional appendix added with guidance 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.

ICS Tailoring Guidance

- In situations where the ICS cannot support, or the organization determines it is not advisable to implement particular security controls or control enhancements in an ICS (e.g., performance, safety, or reliability are adversely impacted), the organization provides a complete and convincing rationale for how the selected compensating controls provide an equivalent security capability or level of protection for the ICS and why the related baseline security controls could not be employed.
- In accordance with the Technology-related Considerations of the Scoping Guidance, if automated mechanisms are not readily available, cost-effective, or technically feasible in the ICS, compensating security controls, implemented through nonautomated mechanisms or procedures are employed.
- Compensating controls are not exceptions or waivers to the baseline controls; rather, they are alternative safeguards and countermeasures employed within the ICS that accomplish the intent of the original security controls that could not be effectively employed. Organizational decisions on the use of compensating controls are documented in the security plan for the ICS.

ICS Supplemental Guidance

- Provides additional information on the application of the security controls and control enhancements to ICS and the environments in which ICS operate
- Provides information as to why a particular security control or control enhancement may not be applicable in some ICS environments and may be a candidate for tailoring (i.e., the application of scoping guidance and/or compensating controls)
- ICS Supplemental Guidance does not replace the original Supplemental Guidance

Security Controls & Control Enhancements Likely Candidates For Tailoring (1/2)

CONTRO L NUMBER	CONTROL NAME	TAILORING OPTIONS	
		SCOPING GUIDANC	COMPENSATING CONTROLS
AC-2	Account Management	NO	YES
AC-5	Separation of Duties	NO	YES
AC-6	Least Privilege	NO	YES
AC-7	Unsuccessful Login Attempts	NO	YES
AC-8	System Use Notification	NO	YES
AC-10	Concurrent Session Control	NO	YES
AC-11	Session Lock	NO	YES
AC-17	Remote Access	NO	YES
AC-17 (2)	Remote Access	NO	YES
AC-19	Access Control for Mobile Devices	NO	YES
AU-2	Auditable Events	NO	YES
AU-5	Response to Audit Processing Failure	YES	YES
AU-7	Audit Reduction and Report Generation	YES	YES
AU-12	Audit Generation	NO	YES
AU-12 (1)	Audit Generation	NO	YES
CA-2	Security Assessments	NO	YES

Security Controls & Control Enhancements Likely Candidates For Tailoring (2/2)

CONTROL NUMBE	CONTROL NAME	TAILORING OPTIONS	
		SCOPING	COMPENSATING CONTROLS
CP-4	Contingency Plan Testing and Exercises	NO	YES
CP-4 (1)	Contingency Plan Testing and Exercises	NO	YES
CP-4 (2)	Contingency Plan Testing and Exercises	NO	YES
CP-4 (4)	Contingency Plan Testing and Exercises	NO	YES
CP-7	Alternate Processing Site	NO	YES
IA-2	User Identification & Authentication (Organizational Users)	NO	YES
IA-3	Device Identification and Authentication	NO	YES
MA-4 (3)	Non-Local Maintenance	YES	YES
MP-5 (4)	Media Transport	YES	YES
PE-6 (2)	Monitoring Physical Access	YES	YES
RA-5	Vulnerability Scanning	NO	YES
SC-2	Application Partitioning	YES	YES
SC-3	Security Function Isolation	NO	YES
SC-7 (6)	Boundary Protection	YES	NO
SC-7 (8)	Boundary Protection	YES	YES
SC-10	Network Disconnect	NO	YES
SI-2 (1)	Flaw Remediation	YES	YES
SI-3 (1)	Malicious Code Protection	YES	YES
SI-8 (1)	Spam Protection	YES	YES

ICS Supplements to the Security Control Baselines

- Recommended ICS supplements **(highlighted in bold text)** to the security control baselines

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
Access Control				
AC-3	Access Enforcement	AC-3	AC-3 **(2)**‡	AC-3 **(2)** ‡
Physical and Environmental Protection				
PE-9	Power Equipment and Power Cabling	Not Selected	PE-9 **(1)**	PE-9 **(1)**
PE-11	Emergency Power	**PE-11**	PE-11 **(1)**	PE-11 (1) **(2)**
System and Communications Protection				
SC-24	Fail in known state	Not Selected	**SC-24**	SC-24
System and Information Integrity				
SI-13	Predictable Failure Prevention	Not Selected	Not Selected	**SI-13**

‡ Control moved to base set (Appendix F)

Section-by-Section Control Example — IR-6 Incident Reporting (1/2)

- Control: The organization:
  a) Requires personnel to report suspected security incidents to the organizational incident response capability within [*Assignment: organization-defined time-period*]; and
  b) Reports security incident information to designated authorities.
- Supplemental Guidance: The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. The types of security incidents reported, the content and timeliness of the reports, and the list of designated reporting authorities are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Current federal policy requires that all federal agencies (unless specifically exempted from such requirements), report security incidents to the United States Computer Emergency Readiness Team (US-CERT) within specified timeframes designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling. Related controls: IR-4, IR-5.

Section-by-Section Control Example — IR-6 Incident Reporting (2/2)

- Control Enhancements:
  1) **The organization employs automated mechanisms to assist in the reporting of security incidents.**
  2) The organization reports information system weaknesses, deficiencies, and/or vulnerabilities associated with reported security incidents to appropriate organizational officials.
- References: NIST Special Publication 800-61: Web: WWW.US-CERT.GOV.
- ICS Supplemental Guidance: The United States Computer Emergency Readiness Team (US-CERT) maintains the ICS Security Center at http://www.uscert.gov/control_systems.
- ICS References: NIST Special Publication 800-82.

Example ICS Supplemental Guidance — CA-2 Security Assessments

ICS Supplemental Guidance:

Assessments are performed and documented by qualified assessors (i.e., experienced in assessing ICS) authorized by the organization. The organization ensures that assessments do not interfere with ICS functions. The individual/group conducting the assessment fully understands the organizational information security policies and procedures, the 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 an assessment can be conducted. If an ICS must be taken off-line to conduct an assessment, the assessment is scheduled to occur during planned ICS outages whenever possible. In situations where the organization cannot, for operational reasons, conduct a live assessment of a production ICS, the organization employs compensating controls (e.g., providing a replicated system to conduct the assessment) in accordance with the general tailoring guidance.

Example ICS Supplemental Guidance — SC-13 Use Of Cryptography

ICS Supplemental Guidance:

The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS.

Example ICS Supplemental Guidance — CP-2 Contingency Plan

ICS Supplemental Guidance:

The organization defines contingency plans for categories of disruptions or failures. In the event of a loss of processing within the ICS or communication with operational facilities, the ICS executes predetermined procedures (e.g., alert the operator of the failure and then do nothing, alert the operator and then safely shut down the industrial process, alert the operator and then maintain the last operational setting prior to failure). Consideration is given to restoring system state variables as part of restoration (e.g., valves are restored to their original settings prior to the disruption).

ICS Baseline Supplement — AC-3 Access Enforcement

- Control: The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.
- Control Enhancement added to ICS moderate baseline
  - (2) The information system enforces dual authorization, based on organizational policies and procedures for [*Assignment: organization-defined privileged commands*].
  - Enhancement Supplemental Guidance: Dual authorization mechanisms require two forms of approval to execute. The organization does not employ dual authorization mechanisms when an immediate response is necessary to ensure public and environmental safety.
  - ICS Supplemental Guidance: The organization ensures that access enforcement mechanisms do not adversely impact the operational performance of the ICS.

ICS Baseline Supplement – SC-24 Fail in Known State

- Added to High Baseline; ICS Moderate Baseline
- Control: The information system fails to a [*Assignment: organization-defined known-state*] for [*Assignment: organization-defined types of failures*] preserving [*Assignment: organization-defined system state information*] in failure.
  - Supplemental Guidance: Failure in a known state can address safety or security in accordance with the mission/business needs of the organization. Failure in a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the information system or a component of the system. Failure in a known safe state helps prevent systems from failing to a state that may cause injury to individuals or destruction to property. Preserving information system state information facilitates system restart and return to the operational mode of the organization with less disruption of mission/business processes.

ICS Concern in Main Control Catalog — CP-10 Information System Recovery And Reconstitution

- Included in low baseline
- Control: The organization provides for the recovery and reconstitution of the information system to a known ~~secure~~ state after a disruption, compromise, or failure.

ICS Baseline Supplement –
SI-13 Predictable Failure Prevention

- Added to ICS high baseline. Based on actual vendor bulletin that DCS crashes after 70.96 days
- Control: The organization:
  a) Protects the information system from harm by considering mean time to failure for [*Assignment: organization-defined list of information system components*] in specific environments of operation; and
  b) Provides substitute information system components, when needed, and a mechanism to exchange active and standby roles of the components.
  - Supplemental Guidance: While mean time to failure is primarily a reliability issue, this control focuses on the potential failure of specific components of the information system that provide security capability. Mean time to failure rates are defendable and based on considerations that are installation-specific, not industry average. The transfer of responsibilities between active and standby information system components does not compromise safety, operational readiness, or security (e.g., state variables are preserved). The standby component is available at all times except where a failure recovery is in progress, or for maintenance reasons.

Key Take Away

- NIST SP 800-53 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.

- NIST SP 800-53, Revision 3 available at:
  - http://csrc.ncsl.nist.gov/publications/PubsSPs.html

Federal ICS using NIST SP 800-53

- Bonneville Power Administration (BPA)
- Southwestern Power Administration (SWPA)
- Tennessee Valley Authority (TVA)
- Western Area Power Administration (WAPA)
- Federal Aviation Administration (FAA)
- Department of the Interior, Bureau of Reclamation

Major ICS Security Objectives

- **Restricting logical access to the ICS network and network activity**
  - This includes using a demilitarized zone (DMZ) network architecture with firewalls to prevent network traffic from passing directly between the corporate and ICS networks, and having separate authentication mechanisms and credentials for users of the corporate and ICS networks. The ICS should also use a network topology that has multiple layers, with the most critical communications occurring in the most secure and reliable layer.
- **Restricting physical access to the ICS network and devices**
  - Unauthorized physical access to components could cause serious disruption of the ICS's functionality. A combination of physical access controls should be used, such as locks, card readers, and/or guards.

Major ICS Security Objectives

- **Protecting individual ICS components from exploitation**
  - This includes deploying security patches in as expeditious a manner as possible, after testing them under field conditions; disabling all unused ports and services; restricting ICS user privileges to only those that are required for each person’s role; tracking and monitoring audit trails; and using security controls such as antivirus software and file integrity checking software where technically feasible to prevent, deter, detect, and mitigate malware.
- **Maintaining functionality during adverse conditions**
  - This involves designing the ICS so that each critical component has a redundant counterpart. Additionally, if a component fails, it should fail in a manner that does not generate unnecessary traffic on the ICS or other networks, or does not cause another problem elsewhere, such as a cascading event.

Summary

- The most successful method for securing an ICS is to gather industry recommended practices and engage in a ***proactive, collaborative effort*** between management, the controls engineer and operator, the IT department, the physical security department, and a trusted automation advisor. This team should draw upon the wealth of information available from ongoing federal government, industry group, vendor and standards organizational activities.

NIST ICS Security Project Contact Information

Project Leader:

Dr. Ronald Ross, (301) 975-5390, Ronald.Ross@nist.gov

Technical Lead:

Keith Stouffer, (301) 975-3877, Keith.Stouffer@nist.gov

Project Staff:

Dr. Marshall Abrams, (703) 983-6938, abrams@mitre.org

Dr. Stu Katzke, (301) 785-2939, katzke@ieee.org

Project email: 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
NIST Special Publications	http://csrc.nist.gov/publications/PubsSPs.html