engineering laboratory

Cybersecurity for Smart Manufacturing Research at NIST

Keith Stouffer
Project Leader,
Cybersecurity for
Smart Manufacturing
Systems

Engineering Lab, NIST

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

National Institute of Standards and Technology (NIST)

- 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
- 2,700 guest researchers
- 1,300 field staff in partner organizations
- Two main locations: Gaithersburg, MD, and Boulder, CO
- $840 million annual budget
- NIST Laboratories
  – National measurement standards
- Manufacturing Extension Partnership
  – Centers nationwide to help small and medium sized manufacturers

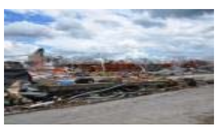
NIST Priority Research Areas

Advanced Manufacturing

IT and Cybersecurity

Healthcare

Forensic Science



Disaster Resilience

Cyberphysical Systems

Advanced Communications

Manufacturing Cybersecurity Research

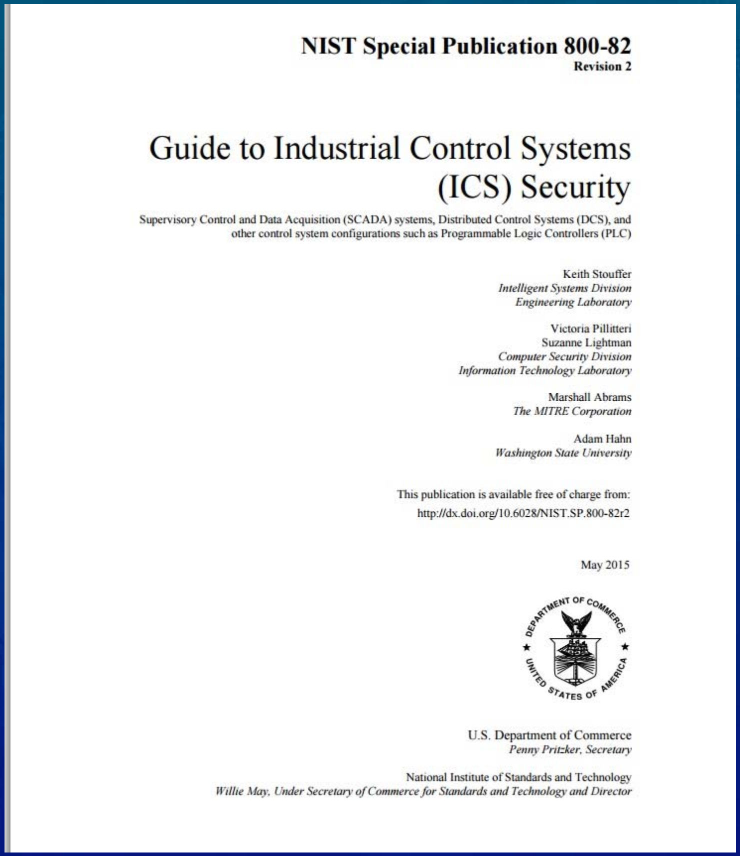
- Current efforts are focused on the development of a cybersecurity risk management framework with supporting guidelines, methods, metrics and tools to enable manufacturers to quantitatively assess the cyber risk to their systems, and develop and deploy a cybersecurity program to mitigate their risk, while addressing the demanding performance, reliability, and safety requirements of manufacturing systems.

ICS Security Standards and Guidelines Strategy

- EL and ITL have been collaborating since 2006 to add control systems domain expertise to:
  - Already available IT security Risk Management Framework to provide workable, practical solutions for control systems
- Results are specific cautions, recommendations & requirements for applying security capabilities to control systems
  - Augmentation of NIST SP 800-53 *Recommended Security Controls for Federal Information Systems*
  - NIST SP 800-82 *Guide to Industrial Control System (ICS) Security*
- Deploy security solution based on potential impact
  - Not a one size fits all solution

NIST SP 800-82

- Guide to Industrial Control Systems Security
  - Provides guidance for establishing secure ICS, while addressing unique performance, reliability, and safety requirements, including implementation guidance for NIST SP 800-53 controls
- Initial draft - September 2006
- Revision 1 - May 2013
- Revision 2 - May 2015
- Downloaded over 3,000,000 times since initial release in 2006 and is heavily referenced by the public and private industrial control community


NIST Special Publication 800-82
Revision 2

Guide to Industrial Control Systems (ICS) Security

Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)

Keith Stouffer
Intelligent Systems Division
Engineering Laboratory

Victoria Pillitteri
Suzanne Lightman
Computer Security Division
Information Technology Laboratory

Marshall Abrams
The MITRE Corporation

Adam Hahn
Washington State University

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-82r2

May 2015

DEPARTMENT OF COMMERCE ★ UNITED STATES OF AMERICA ★

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

NIST SP 800-82, Revision 2

- Content
  - Overview of ICS
  - ICS Risk Management and Assessment
  - ICS Security Program Development and Deployment
  - ICS Security Architecture
  - Applying Security Controls to ICS
  - Threat Sources, Vulnerabilities and Incidents
  - Current Activities in Industrial Control Systems Security
  - ICS Security Capabilities and Tools
  - ICS Overlay for NIST SP 800-53, Rev 4 security controls

Major ICS Security Objectives

- **Restrict logical access to the ICS network and network activity**
  - Demilitarized zone (DMZ) network architecture
  - Separate authentication mechanisms and credentials for users of the corporate and ICS networks.
  - Network topology that has multiple layers, with the most critical communications occurring in the most secure and reliable layer.
- **Restrict physical access to the ICS network and devices**
  - Unauthorized physical access to components could cause serious disruption of the ICS's functionality.
  - Combination of physical access controls should be used, such as locks, card readers, and/or guards.

Major ICS Security Objectives

- **Protect individual ICS components from exploitation**
  - Deploy security patches in as expeditious a manner as possible
  - Disable unused ports and services
  - Restrict ICS user privileges to only those that are required
  - Tracking and monitor audit trails
  - Implement antivirus and file integrity checking software where feasible to prevent, deter, detect, and mitigate malware
- **Maintain functionality during adverse conditions**
  - Design ICS so that critical components have redundant counterparts
  - Component failure should not generate unnecessary traffic on the ICS or other networks, or should not cause another problem elsewhere, such as a cascading event

Major ICS Security Objectives

- **Deploy security solution based on potential impact**
  - Not a one size fits all solution
- **Continuous monitoring**
  - Security is not a once and done exercise
  - Continuously monitor risk
    - Continuously monitor threats
    - Continuously monitor and mitigate vulnerabilities
  - Continuously monitor system boundaries
  - Continuously monitor ingress and egress traffic
  - Continuously update security controls

ICS Overlay

- The ICS overlay is a partial tailoring of the controls and three control baselines in SP 800-53, Revision 4, and adds supplementary guidance specific to ICS.
- The concept of overlays is introduced in Appendix I of SP 800-53, Revision 4.
- The ICS overlay is intended to be applicable to all ICS systems in all industrial sectors. Further tailoring can be performed to add specificity to a particular sector (e.g., manufacturing).
- The ICS overlay is included as Appendix G in NIST SP 800-82, Revision 2.

Cybersecurity Framework Profile

- Develop manufacturing implementation (Profile) of the Cybersecurity Framework (CSF) using NIST SP 800-82, Revision 2 for controls
- Implement CSF Manufacturing Profile in the Cybersecurity for Smart Manufacturing Testbed
- Measure performance impact of various cybersecurity solutions to meet the CSF Profile
- Develop guidance on how to implement the CSF in manufacturing environments **without having negative performance impacts**

Cybersecurity Framework Components

Framework Profile

Aligns industry standards and best practices to the Framework Core in a particular implementation scenario

Supports prioritization and measurement while factoring in business needs

Framework Core

Cybersecurity activities and informative references, organized around particular outcomes

Enables communication of cyber risk across an organization

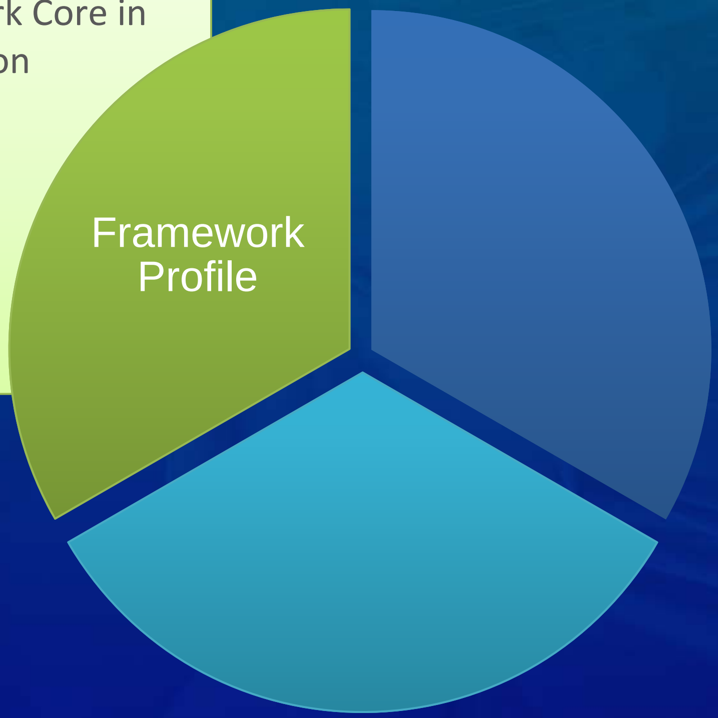
Framework Implementation Tiers

Describes how cybersecurity risk is managed by an organization and degree the risk management practices exhibit key characteristics

Cybersecurity Framework Profile

Aligns industry standards and best practices to the Framework Core in a particular implementation scenario

Supports prioritization and measurement while factoring in business needs



Develop and Implement a Manufacturing Profile of the Cybersecurity Framework

Framework Core

Cybersecurity Framework Component

	Functions	Categories	Subcategories	Informative References
What processes and assets need protection?	IDENTIFY			
What safeguards are available?	PROTECT			
What techniques can identify incidents?	DETECT			
What techniques can contain impacts of incidents?	RESPOND			
What techniques can restore capabilities?	RECOVER			

Cybersecurity Framework Core

Function	Category	ID
Identify	Asset Management	**ID.AM**
	Business Environment	**ID.BE**
	Governance	**ID.GV**
	Risk Assessment	**ID.RA**
	Risk Management Strategy	**ID.RM**
Protect	Access Control	**PR.AC**
	Awareness and Training	**PR.AT**
	Data Security	**PR.DS**
	Information Protection Processes & Procedures	**PR.IP**
	Maintenance	**PR.MA**
	Protective Technology	**PR.PT**
Detect	Anomalies and Events	**DE.AE**
	Security Continuous Monitoring	**DE.CM**
	Detection Processes	**DE.DP**
Respond	Response Planning	**RS.RP**
	Communications	**RS.CO**
	Analysis	**RS.AN**
	Mitigation	**RS.MI**
	Improvements	**RS.IM**
Recover	Recovery Planning	**RC.RP**
	Improvements	**RC.IM**
	Communications	**RC.CO**

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	COBIT 5 APO01.02, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	COBIT 5 APO02.06, APO03.01 NIST SP 800-53 Rev. 4 PM-8
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	COBIT 5 APO02.01, APO02.06, APO03.01 ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 NIST SP 800-53 Rev. 4 PM-11 SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established	ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14

Profile

Cybersecurity Framework Component

Ways to think about a Profile:

- A customization of the Core for a given sector, subsector, or organization
- A fusion of business/mission logic and cybersecurity outcomes

Identify
Protect
Detect
Respond
Recover

- An alignment of cybersecurity requirements with operational methodologies
- A basis for assessment and expressing target state
- A decision support tool for cybersecurity risk management

Draft CSF Manufacturing Profile

Table of Contents

DRAFT

Public comment period:

September 7, 2016 –
November 4, 2016

http://csrc.nist.gov/cyberframework/documents/csf-manufacturing-profile-draft.pdf

NIST Cybersecurity for Smart Manufacturing Systems Testbed

- Goal of the testbed is to measure the performance of ICS when instrumented with cybersecurity protections in accordance with practices prescribed by national and international standards and guidelines such as Cybersecurity Framework, SP 800-82 and ISA/IEC 62443
- Research areas include
  - Perimeter network security
  - Host-based security
  - User and device authentication
  - Packet integrity and authentication
  - Encryption
  - Zone-based security
  - Field bus (non-routable) protocol security
  - Robust/ fault tolerant systems

Industrial Performance Metrics

Metric	Description
Product Quality	A quantitative measurement of product correctness or purity
Defect Rate	Rate at which a product fails quality control checks due to errors in the manufacturing process.
Defects per unit	Statistical measures of the number of defects per unit
Process Restart Rate	Number of times a process must be restarted in a given time interval.
Variability of On-time Actuation	Statistical measure of time between command and actuation completion.
Steady State Error	Oscillation over variability about a pre-determined set point.
Response Time	A quantitative measurement of time to respond to a perturbation such as a step stimulus.
Process Duration	Length of time to complete a sequence of tasks such as a series of assembly tasks in a robotic assembly system.

Network Performance Metrics

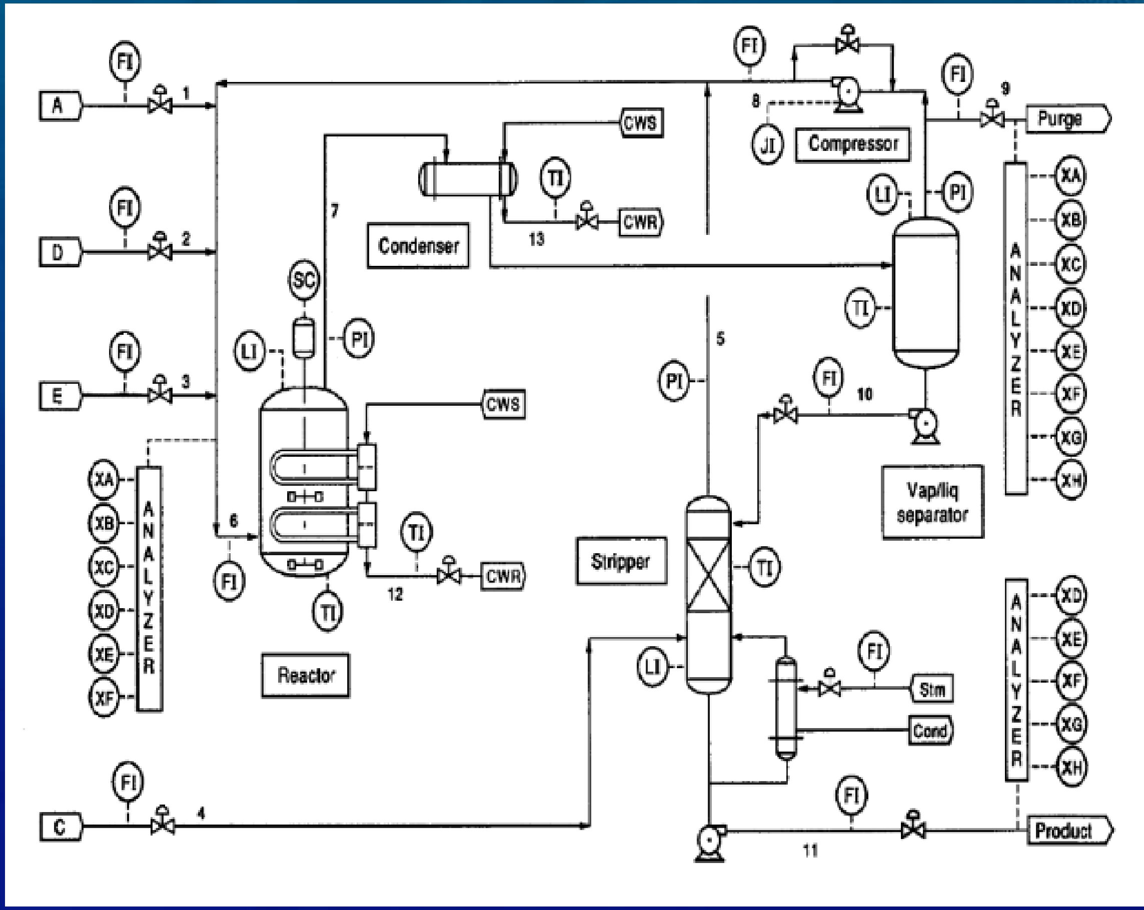
Metric	Description
Information Packet Rate	Rate of information packet flow that is useful to the application measured at the highest observable network layer.
Information Bit Rate	Rate of information bit flow that is useful to the application measured at the highest observable network layer.
Raw Packet Rate	Measured at layer 2 and includes overhead and retries
Raw Bit Rate	Measured at layer 2 and includes overhead and retries
Message Delay (Distribution)	The delay for full messages (multiple packets) to be propagated through the network or network link. Used for long packets measured at the layer in which transport layer packets are reassembled which is usually the application layer.
Packet Delay (Distribution)	The delay for single packets to be propagated through the network or network link.
Packet Delay Jitter	Variation in delay measured over an ensemble of packets.
Processing Delay	Delay introduced by network interconnect devices such as switches and routers
Queuing Delay	Amount of time a packet spending in the input queue before being processed
Propagation Delay	The amount of time a quanta of information takes to travel between transmitter and receiver
Packet Collisions	Number of collisions typically reported by layer 2 devices
Packet error rate	Rate of packet errors measured at the transport layer
Packet loss rate	Rate of packet loss measured at the transport layer
Packet Size (Distribution)	Distribution of the size of packets transmitted across the network.
Measured Determinism Boundaries	Measured points of real-time determinism failure

Testbed Scenarios

- Continuous Processes
  - Chemical Processing
- Advanced Discrete Processes
  - Dynamic Robotic Assembly
  - Additive Manufacturing
- Distributed Operations
  - Smart Grid
  - Smart Transportation

Process Control Scenario: The Tennessee Eastman Process

- Continuous process
- Dynamic Oscillations
- Integrated safety system
- Multiple Protocols
  - EtherNET/IP
  - OPC
  - DeviceNet
  - HART
- Hardware-in-the-loop
  - PLC-based control



Dynamic Robotic Assembly

- Discrete process
- Cooperative robotics
- Dynamic Planning
- Integrated safety system
- Computer Vision
- Embedded control
- A variety of protocols including EtherCAT

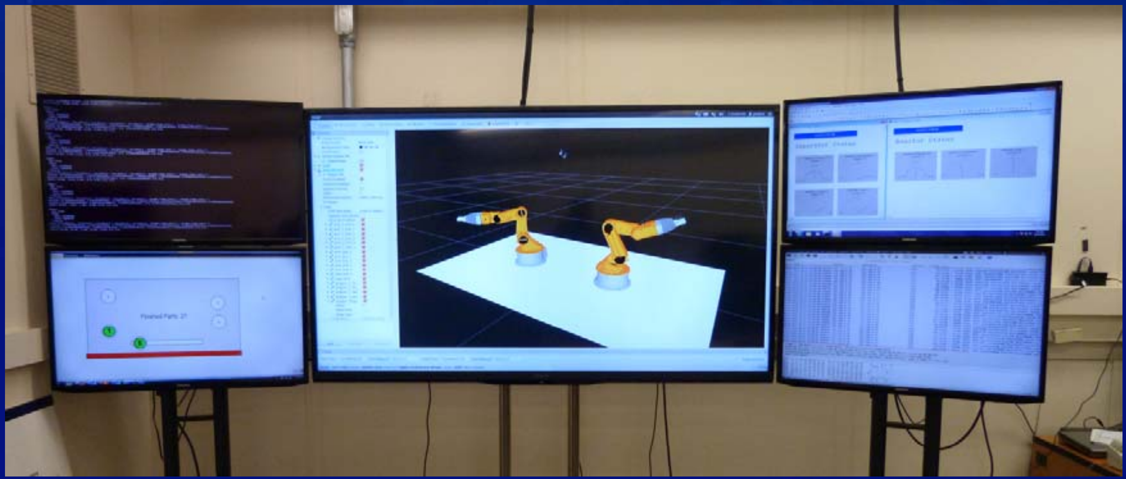
NIST Cybersecurity for Smart Manufacturing Systems Testbed

Collaborative Robotics Enclave

Process Control Enclave

Measurement Enclave

NIST Cybersecurity for Smart Manufacturing Systems Testbed



Contact Info

Keith Stouffer

301 975 3877
keith.stouffer@nist.gov

Engineering Laboratory
National Institute of Standards and Technology
100 Bureau Drive, Mail Stop 8230
Gaithersburg, MD 20899-8230