NIST Cybersecurity Framework – Manufacturing Implementation

Keith Stouffer
Project Leader,
Cybersecurity for
Smart Manufacturing
Systems

Engineering Lab, NIST

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

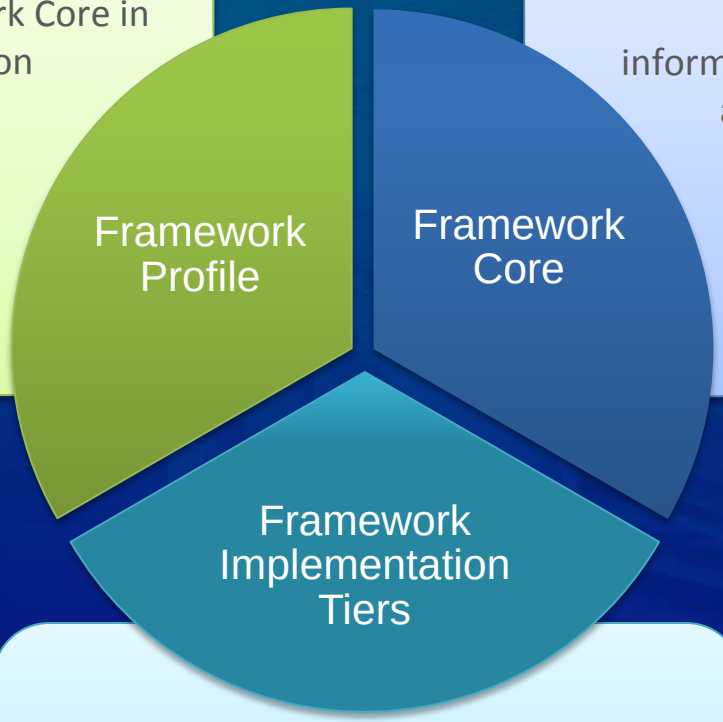
Manufacturing Cybersecurity Research at NIST

- Develop a Manufacturing Cybersecurity Framework (CSF) Profile for various manufacturing scenarios
- Implement Manufacturing CSF Profile in the NIST Cybersecurity for Smart Manufacturing Testbed
- Measure performance impact of various cybersecurity solutions to meet the Manufacturing CSF Profile
- Develop guidance on how to implement the NIST CSF in manufacturing environments without having negative performance impacts
- Collaborate with Manufacturing Extension Partnership (MEP) and National Cybersecurity Center of Excellence (NCCoE) to develop cybersecurity guidance for small and medium sized manufacturers that is actionable and not overwhelming

Cybersecurity Framework Components

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

Supports prioritization and measurement while factoring in business needs



Cybersecurity activities and informative references, organized around particular outcomes

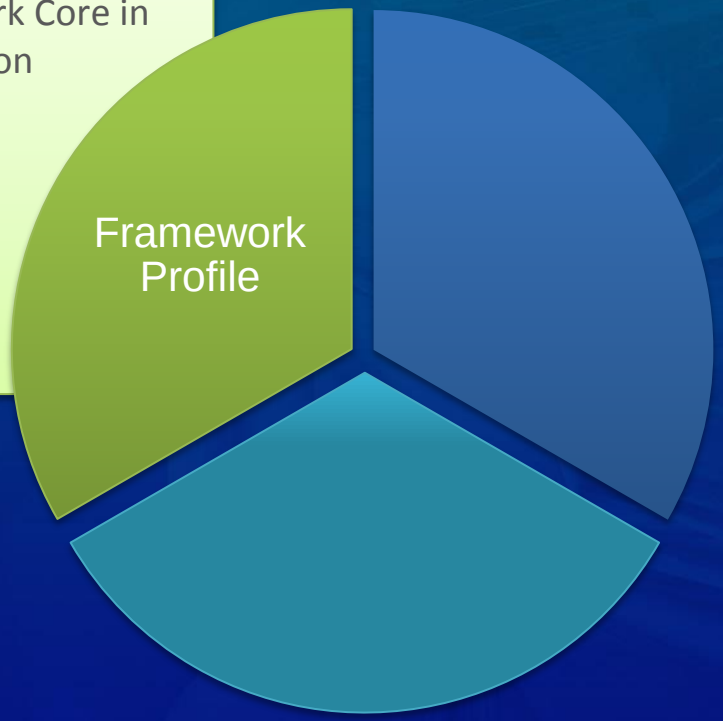
Enables communication of cyber risk across an organization

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

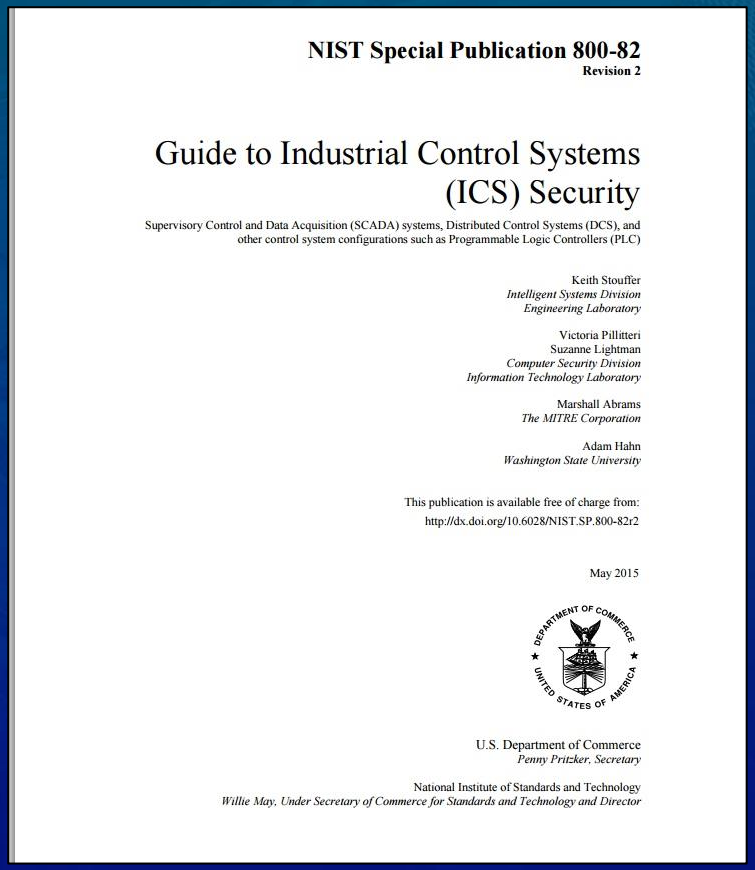
Supports prioritization and measurement while factoring in business needs



Develop and Implement a Manufacturing Profile of the Cybersecurity Framework

NIST Special Publication 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



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

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 Special Publication 800-82

- Guide to Industrial Control Systems Security
  - Provide guidance for establishing secure ICS, including implementation guidance for NIST SP 800-53 security controls
- 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
- Downloaded over 3,000,000 times since 2006 initial release and is heavily referenced by the public and private ICS security community worldwide

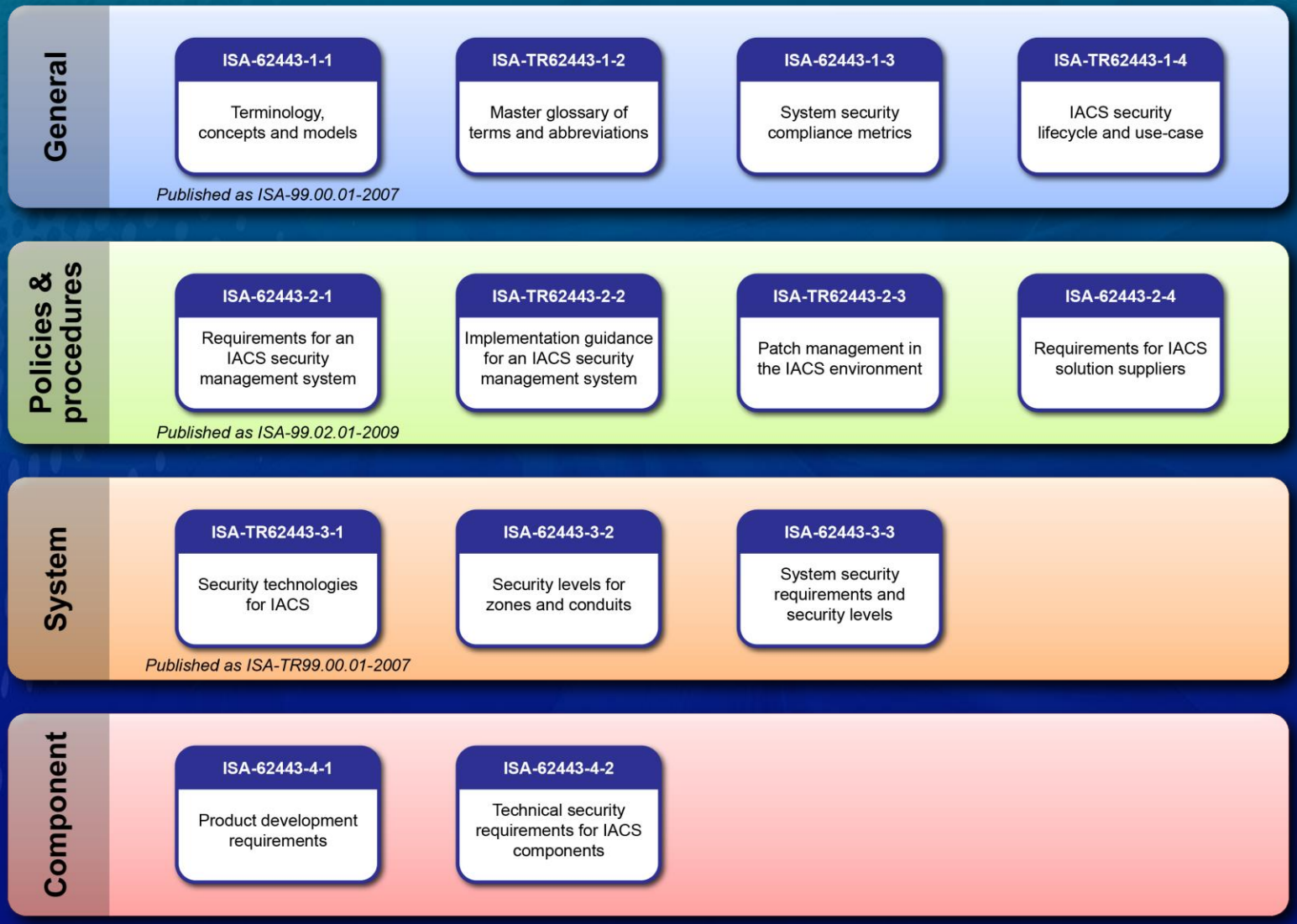
ICS Overlay

- 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.

ISA99 Committee

- The International Society of Automation (ISA) Committee on Security for Industrial Automation & Control Systems (ISA99)
  - 500+ members
  - Representing companies across all sectors, including:
    - Chemical Processing
    - Petroleum Refining
    - Food and Beverage
    - Energy
    - Pharmaceuticals
    - Water
    - Manufacturing

The ISA/IEC-62443 Series



Facility Control Systems

- Although NIST SP 800-82 provides guidance for securing ICS, other types of control systems share similar characteristics and many of the recommendations from the guide are applicable and could be used as a reference to protect such systems against cybersecurity threats. For example, although many building, transportation, medical, security and logistics systems use different protocols, ports and services, and are configured and operate in different modes than ICS, they share similar characteristics to traditional ICS.

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 the NIST 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

NIST Cybersecurity for Smart Manufacturing Systems Testbed

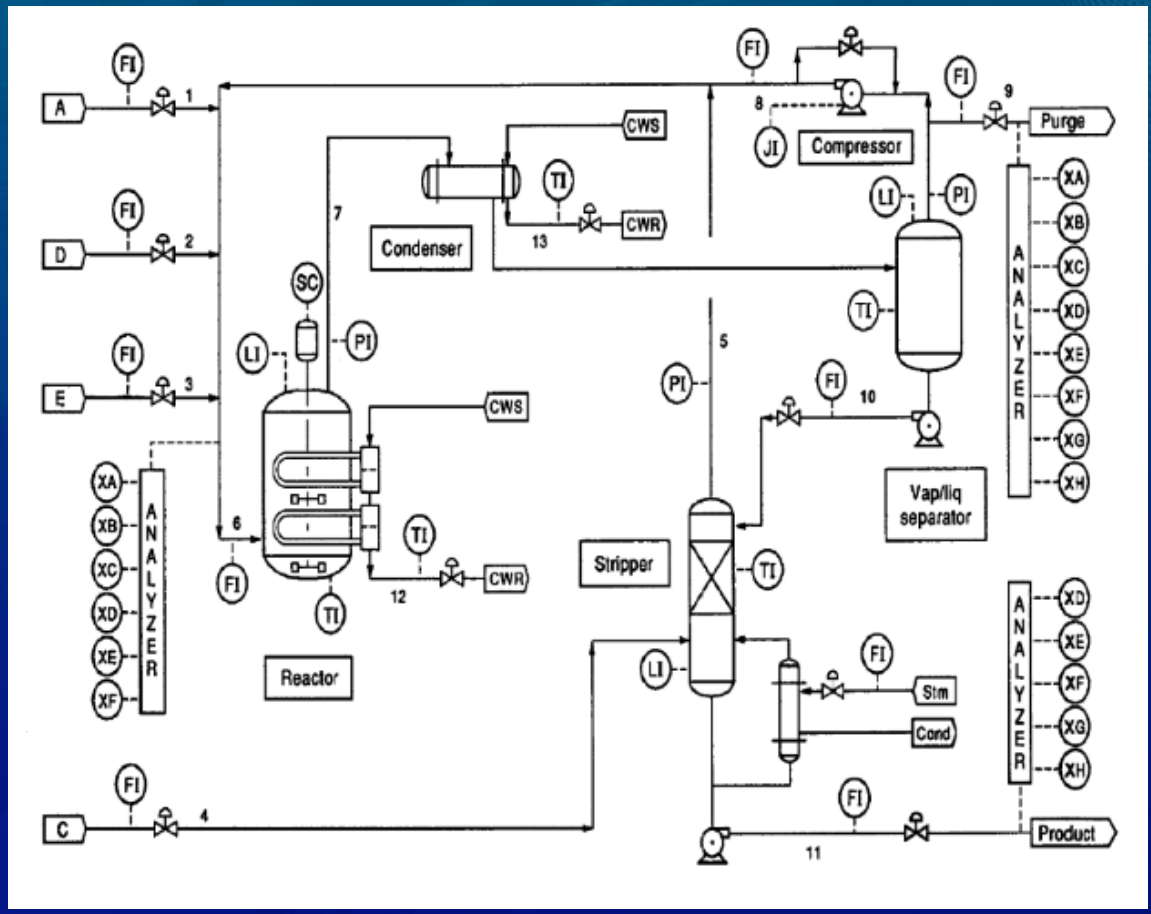
- Reconfigurable nature of testbed will allow for researching various implementations for each scenario
  - Process Control
  - Collaborative Robotics
  - Additive Manufacturing
  - Assembly
- Research outcomes will be used to develop guidance for cost effectively implementing the NIST CSF in manufacturing environments without having negative performance impacts on the systems

Testbed Scenarios

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

Process Control Scenario: The Tennessee Eastman Process

- Continuous process
- Dynamic Oscillations
- Integrated safety system
- Multiple Protocols
  - EtherNET/IP
  - OPC
  - DeviceNet
- 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

Transportation

- Railway
  - Track sensing & control
  - Train Scheduling
  - Locomotive
- Automotive
  - Vehicle-vehicle communications
  - Infrastructure sensing & control

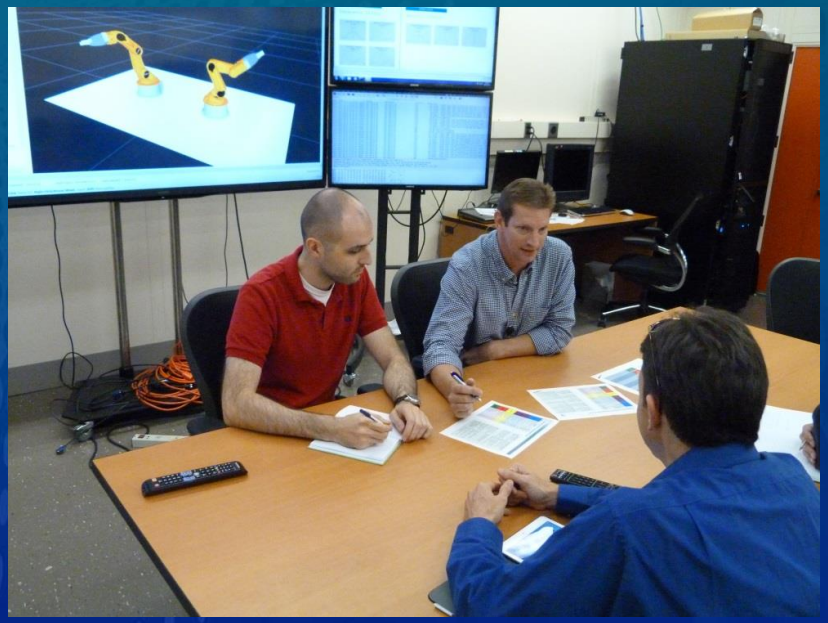
NIST Cybersecurity for Smart Manufacturing Systems Testbed

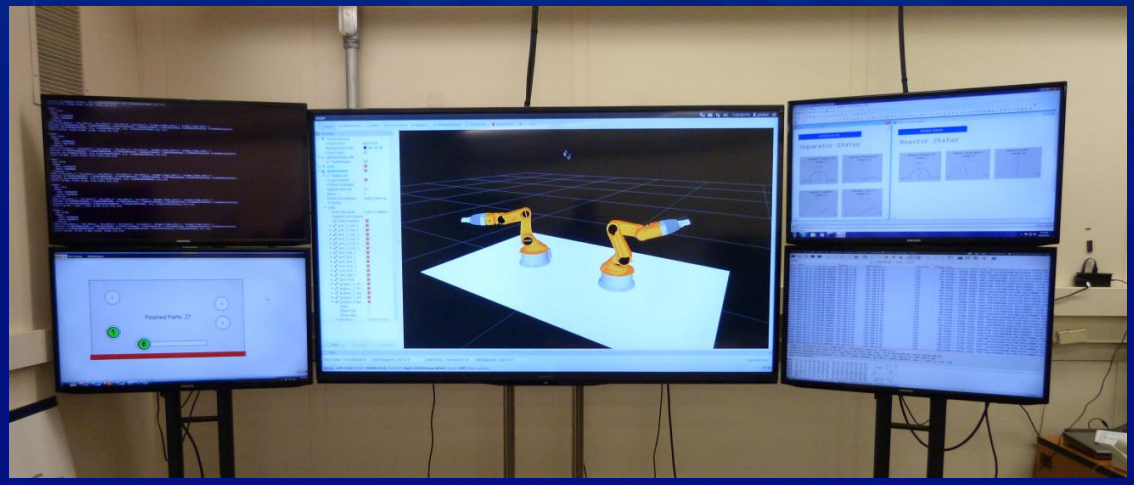
Collaborative Robotics Enclave

Process Control Enclave

Measurement Enclave

NIST Cybersecurity for Smart Manufacturing Systems Testbed





NIST Virtual Cybernetic Building Testbed (VCBT)

- The VCBT is a whole building emulator designed with enough flexibility to be capable simulating normal operation and a variety of faulty and hazardous conditions that might occur in a building where numerous building control systems are integrated together and with outside entities such as utility providers.
- The VCBT control hardware consists of BACnet products from multiple companies that are used for HVAC control, lighting control, physical access control, and fire detection.

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 USA