



# Hearing Recommendations From U.S. Government Agencies To Ensure Remote Assets Remain As Secure As Possible

Keith Stouffer  
Project Leader,  
Cybersecurity for  
Smart Manufacturing  
Systems

Engineering Lab, NIST



# 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**



Tobias

Assignment

S. Bonn

SP11/17

NIST

Ensurge

Jovan Netic

Chuck Rausin/shutterstock.com



# 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* – ICS Overlay
  - 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



# Low Impact System



# Low Impact ICS

- **Product Examples:** 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



# Moderate Impact ICS

- **Product Examples:** 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 !!!



# High Impact ICS

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

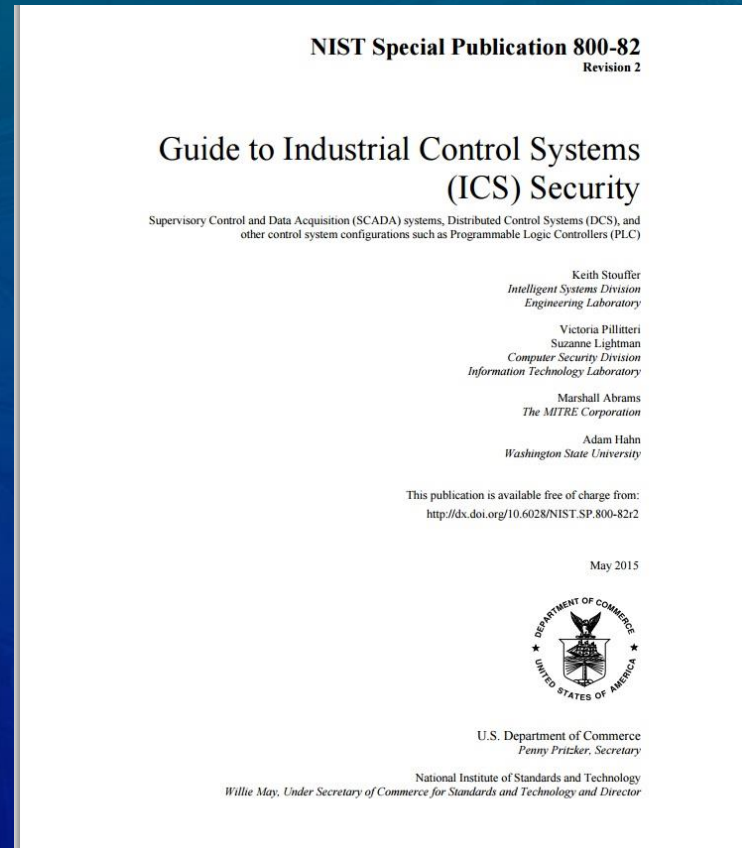


# World Record High Impact System 😊



# 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 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 ICS 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.

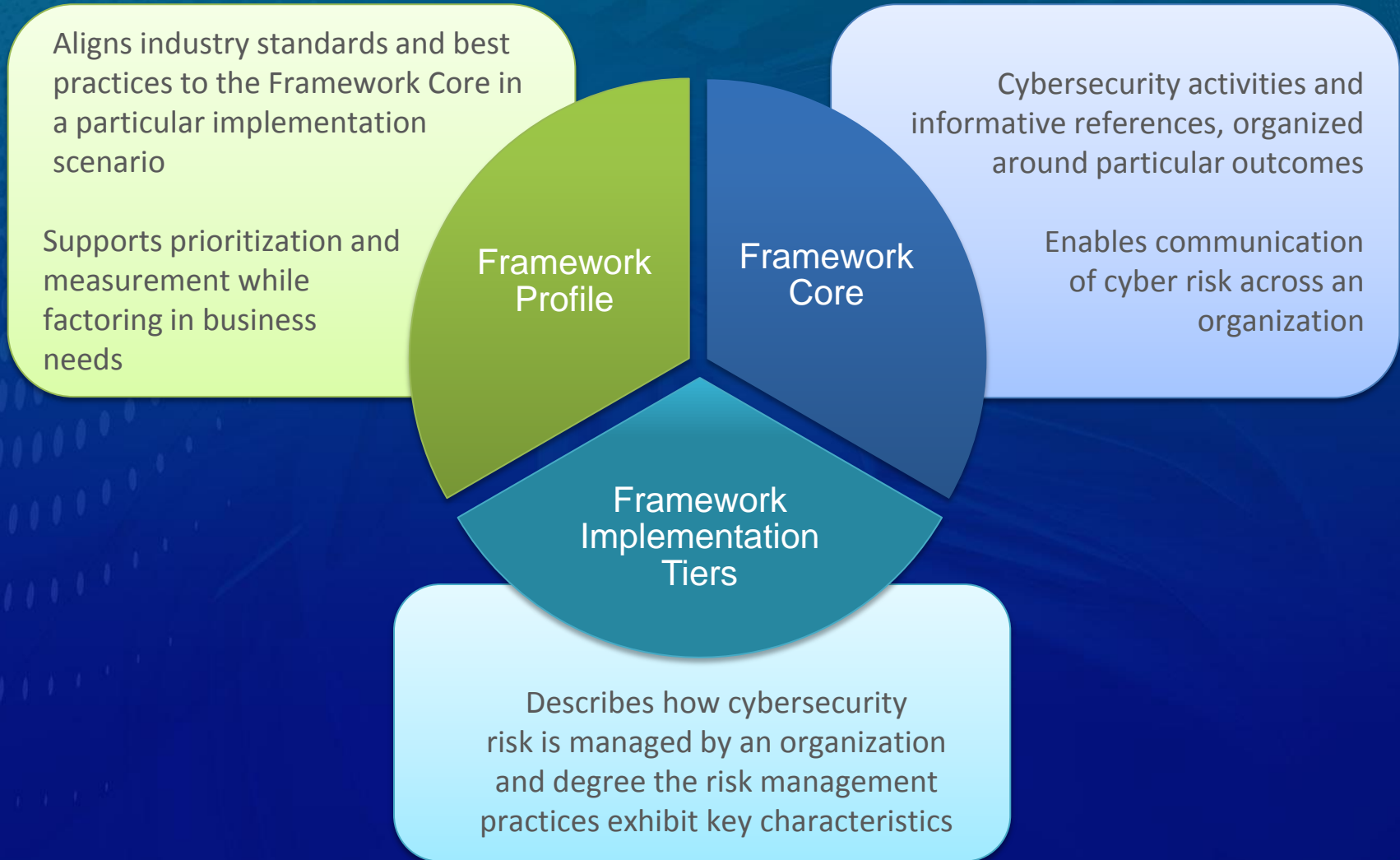


# Next Steps

- Integrate NIST SP 800-82 into cybersecurity tools
  - Cyber Security Evaluation Tool (CSET®). CSET is a DHS product that assists organizations in protecting their key national cyber assets.
  - Electronic Mission Assurance Support Service (eMASS) is the DoD system in which IT system authorizations to operate (ATOs) are issued and tracked.
- Develop manufacturing implementation (Profile) of the NIST Cybersecurity Framework (CSF) using NIST SP 800-82, Rev 2, NIST SP 800-53, Rev 4 and ISA/IEC 62443 as informative references



# Cybersecurity Framework Components



# 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



Framework Profile

Develop and Implement a Manufacturing Profile of the Cybersecurity Framework



# Framework Core

## Cybersecurity Framework Component

What processes and assets need protection?

What safeguards are available?

What techniques can identify incidents?

What techniques can contain impacts of incidents?

What techniques can restore capabilities?

Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
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
<b>ID.BE-1:</b> 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
<b>ID.BE-2:</b> 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
<b>ID.BE-3:</b> 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
<b>ID.BE-4:</b> 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
<b>ID.BE-5:</b> 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
- An alignment of cybersecurity requirements with operational methodologies
- A basis for assessment and expressing target state
- A decision support tool for cybersecurity risk management

Identify

Protect

Detect

Respond

Recover



# Draft CSF Manufacturing Profile

<b>Executive Summary</b> .....	<b>2</b>
<b>1. Introduction</b> .....	<b>3</b>
1.1 Purpose & Scope.....	3
1.2 Audience .....	4
1.3 Document Structure.....	4
<b>2. Overview of Manufacturing Systems</b> .....	<b>5</b>
<b>3. Overview of the Cybersecurity Framework</b> .....	<b>6</b>
3.1 Framework Core .....	6
<b>4. Manufacturing Profile Development Approach</b> .....	<b>8</b>
4.1 The Framework Profile.....	8
<b>5. Manufacturing Business/Mission Objectives</b> .....	<b>9</b>
5.1 Alignment of Subcategories to Meet Mission Objectives .....	9
<b>6. Risk Management</b> .....	<b>14</b>
6.1 Risk Management and the Cybersecurity Framework.....	14
6.2 Manufacturing System Categorization .....	14
6.3 Profile Categorization Supporting Structure.....	16
<b>7. Manufacturing Profile Subcategory Guidance</b> .....	<b>17</b>
<b>Appendix A - Acronyms and Abbreviations</b> .....	<b>44</b>
<b>Appendix B - Glossary</b> .....	<b>45</b>
<b>Appendix C - References</b> .....	<b>46</b>

CSF Manufacturing Profile URL:  
<http://go.usa.gov/cuPpG>



# Profile Implementation

- Implement Manufacturing CSF Profile in the Cybersecurity for Smart Manufacturing Testbed
- Measure performance impact of various cybersecurity solutions to meet the CSF Profile
- Develop data sets on impact of cybersecurity technologies on manufacturing systems
- Develop guidance on how to implement the NIST CSF in manufacturing environments **without having negative performance impacts**



# 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 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



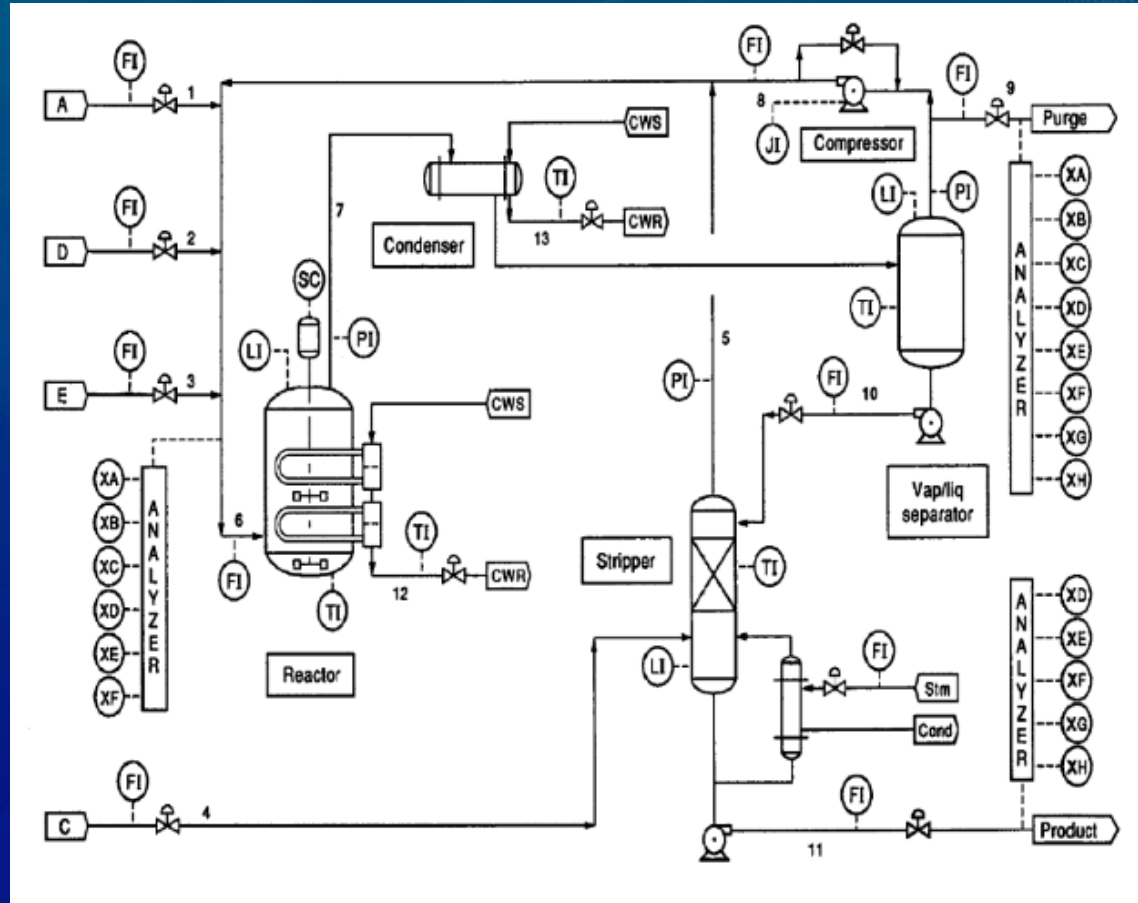
# Testbed Scenarios

- 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



# 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



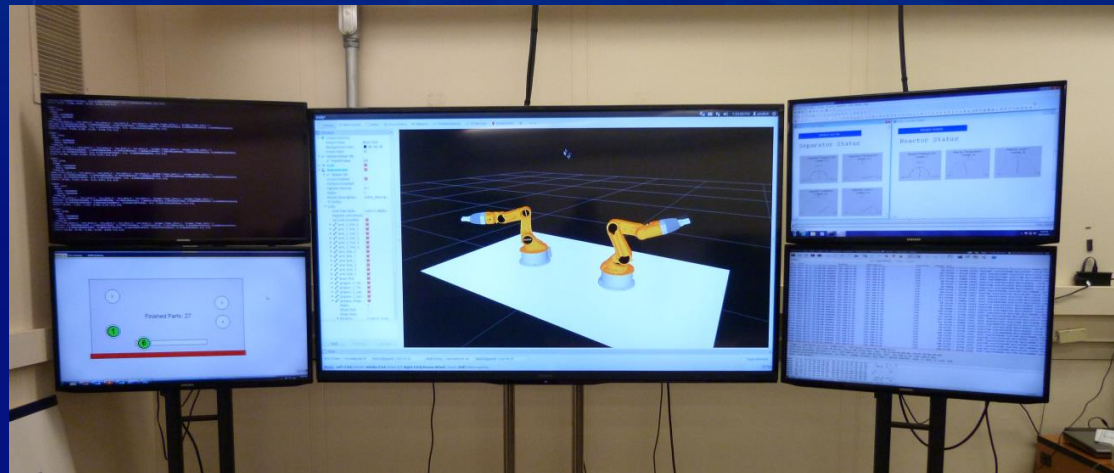
Process  
Control  
Enclave



Measurement  
Enclave



# NIST Cybersecurity for Smart Manufacturing Systems Testbed



# 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

