Cybersecurity for Manufacturing Systems

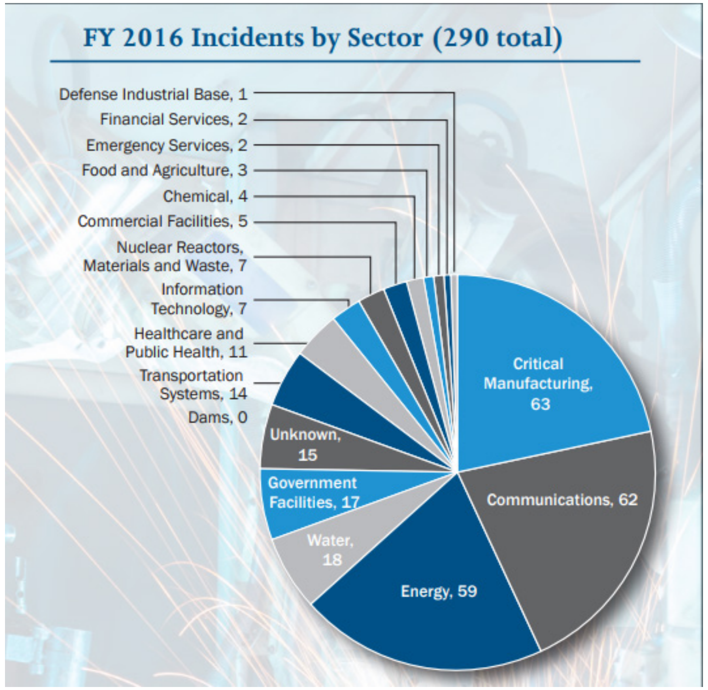
Keith Stouffer

Intelligent Systems Division
Engineering Laboratory
NIST

engineering laboratory

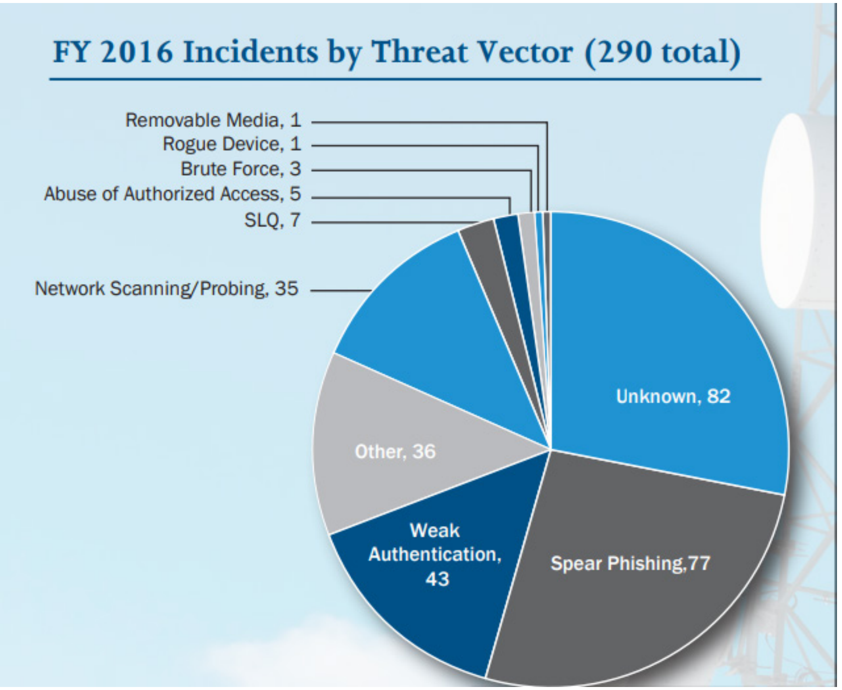
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

FY 2016 Incidents reported to National Cybersecurity and Communication Integration Center (NCCIC)



63 critical manufacturing incidents in FY16 – more than any other sector

Biggest threat vector was spear phishing



- https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_IR_Pie_Chart_FY2016_S508C.pdf

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

Threat - Destructive Malware

- Arguably the biggest threat for most manufacturers
- Examples
  - SoBig – 2003 - Caused $37.1 Billion in damages and is credited with bringing down freight and computer traffic in Washington D.C, as well as Air Canada
  - Stuxnet – 2010 – Took control of Iranian nuclear plant and uranium enrichment plant centrifuges, causing them to eventually fail
  - WannaCry – 2017 – Ransomware attack that infected more than 300,000 computers and shut down automotive plants and hospitals
- Action items to minimize destructive malware and other threats
  - Keep systems patched and updated
  - Implement Application Whitelisting where feasible (e.g., HMIs, database servers)
  - https://ics-cert.us-cert.gov/sites/default/files/documents/Destructive_Malware_White_Paper_S508C.pdf

Configuration and Patch Management

- Adversaries target unpatched systems. A configuration/patch management program centered on the safe importation and implementation of trusted patches will help keep control systems more secure.
- Prioritize patching and configuration management of "PC-architecture" machines used in HMI, database server, and engineering workstation roles, as current adversaries have significant cyber capabilities against these. Infected laptops are a significant malware vector.
- 85 of 295 (29%) incidents reported to ICS-CERT in FY 2015 potentially mitigated by proper configuration and patch management

https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/RP_Patch_Management_S508C.pdf

https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf

Application Whitelisting

- Application Whitelisting (AWL) can detect and prevent attempted execution of malware uploaded by adversaries. The static nature of some systems, such as database servers and human-machine interface (HMI) computers, make these ideal candidates to run AWL. Operators are encouraged to work with their vendors to baseline and calibrate AWL deployments.
- Example: ICS-CERT recently responded to an incident where the victim had to rebuild the network from scratch at great expense. A particular malware compromised over 80 percent of its assets. Antivirus software was ineffective; the malware had a 0 percent detection rate on VirusTotal. AWL would have provided notification and blocked the malware execution.
- 112 of 295 (38%) incidents reported to ICS-CERT in FY 2015 potentially mitigated by AWL
- Guideline for ICS Application Whitelisting

  https://ics-cert.us-cert.gov/sites/default/files/documents/Guidelines%20for%20Application%20Whitelisting%20in%20Industrial%20Control%20Systems_S508C.pdf

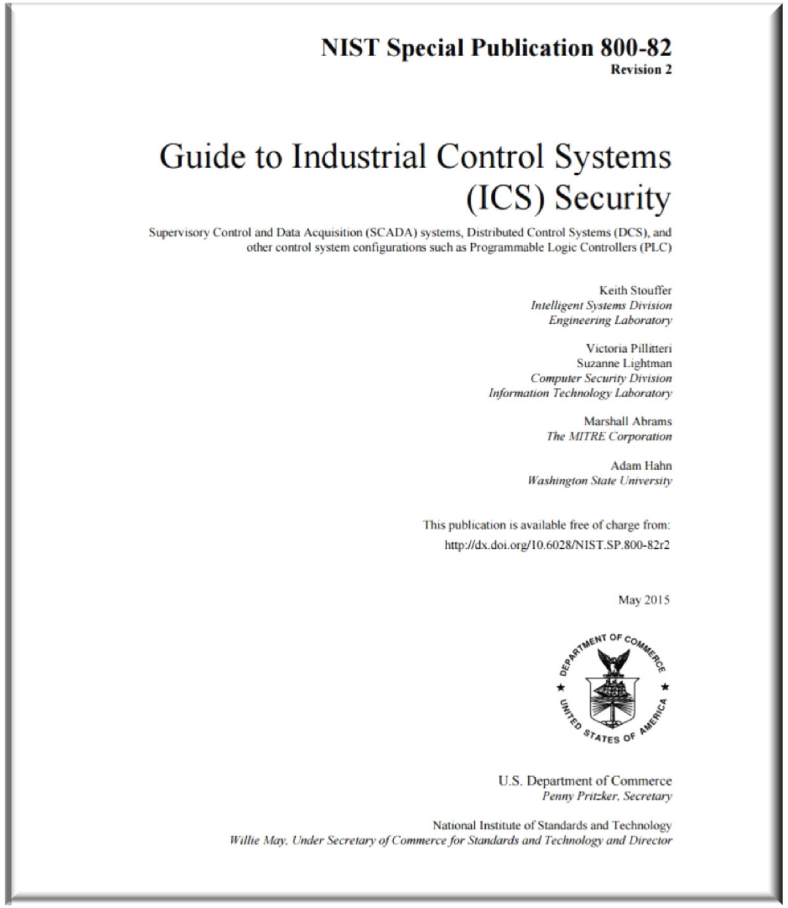
Industrial Control System Cybersecurity Standards and Guidelines

- NIST has been collaborating with industry, government, and academia since 2000 to add control systems domain expertise to already available IT cybersecurity Risk Management Frameworks to provide workable, practical solutions for industrial control systems
- Current efforts are focused on the development of a **comprehensive 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.
  - NIST SP 800-82 *Guide to Industrial Control System (ICS) Security*
  - ISA/IEC 62443 Standards
  - Cybersecurity Framework Manufacturing Profile

NIST SP 800-82

Guide to Industrial Control Systems Security

- Provides a comprehensive cybersecurity approach for securing 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
- 3,000,000+ downloads, 800+ citations,
  de facto worldwide standard/guideline for industrial control system cybersecurity


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

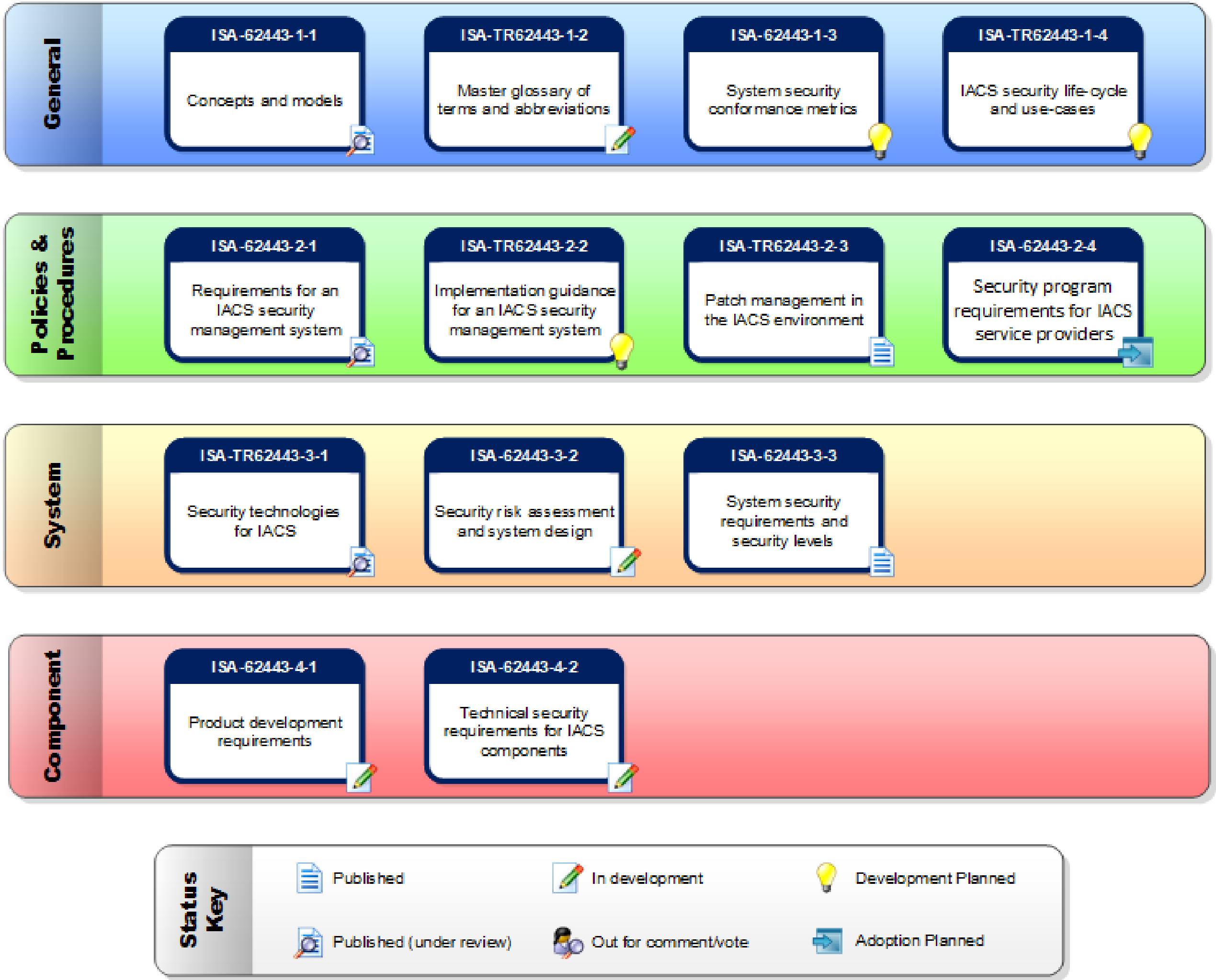
May 2015

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

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

ISA/IEC 62443 http://isa99.isa.org/ISA99%20Wiki/Home.aspx

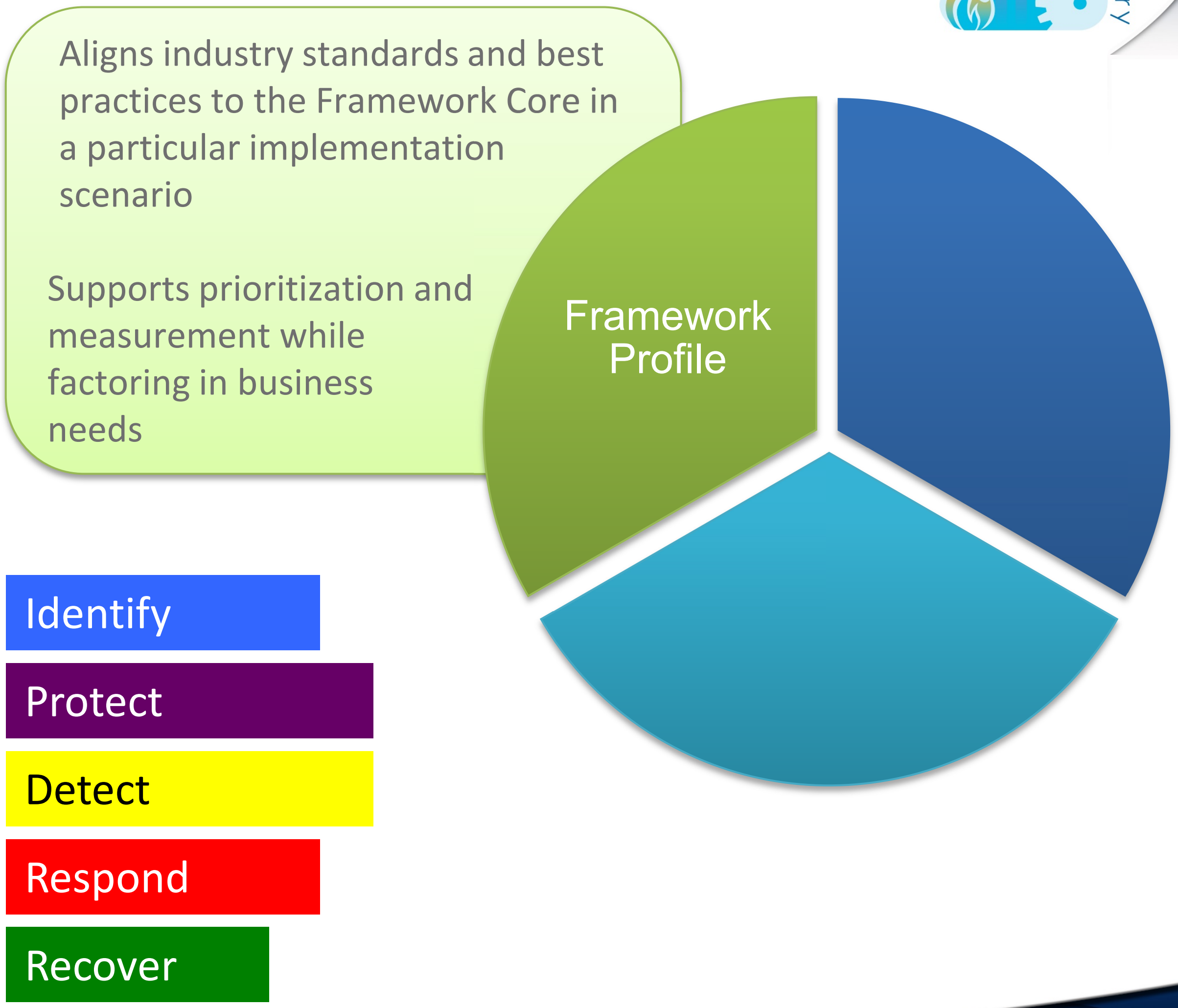


Cybersecurity Framework (CSF) Manufacturing Profile

- Develop manufacturing implementation (Profile) of the CSF using NIST SP 800-82, NIST SP 800-53 and ISA/IEC 62443 as informative references
- Manufacturing Profile is a **Target Profile** of desired cybersecurity outcomes and can be used as a guideline to identify opportunities for improving the current cybersecurity posture of the manufacturing system
- Framework 7 Step Process
  - Step 1: Prioritize and Scope
  - Step 2: Orient
  - Step 3: Create a Current Profile
  - Step 4: Conduct a Risk Assessment
  - **Step 5: Create a Target Profile**
  - Step 6: Determine, Analyze, and Prioritize Gaps
  - Step 7: Implementation Action Plan

Cybersecurity Framework 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



Cybersecurity Framework Manufacturing Profile

NISTIR 8183

Cybersecurity Framework Manufacturing Profile

Keith Stouffer
Timothy Zimmerman
CheeYee Tang
Intelligent Systems Division
Engineering Laboratory

Joshua Lubell
Systems Integration Division
Engineering Laboratory

Jeffrey Cichonski
Applied Cybersecurity Division
Information Technology Laboratory

John McCarthy
Dakota Consulting, Inc.
Silver Spring, Maryland

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8183

September 2017

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology

Table of Contents

http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf

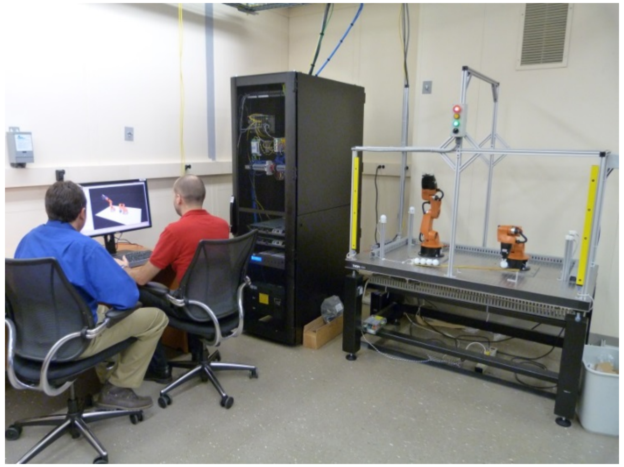
CSF Manufacturing Profile Implementation

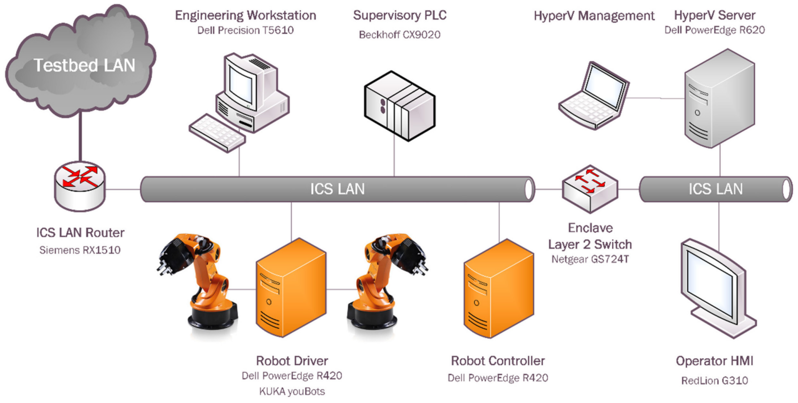
- Implement CSF Manufacturing Profile in the Cybersecurity for Smart Manufacturing Testbed
- Measure manufacturing system network and operational performance impacts when instrumented with cybersecurity protections in accordance with the Manufacturing Profile
- Develop guidance on how to implement the CSF in manufacturing environments **while minimizing negative performance impacts**

Cybersecurity for Manufacturing Systems Testbed

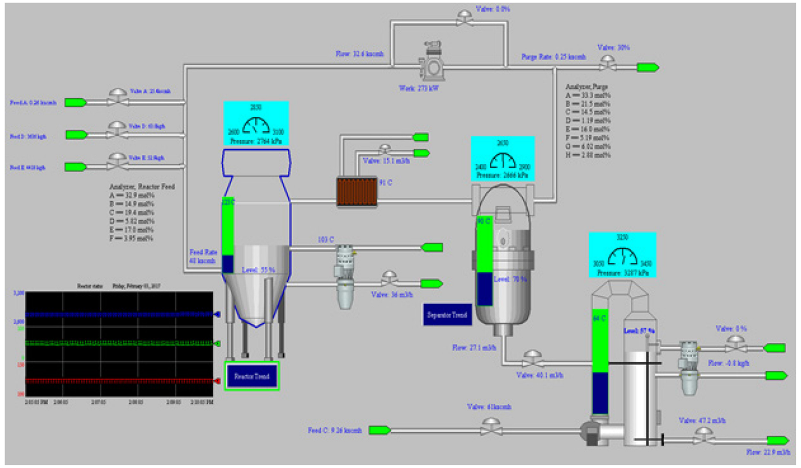
engineering laboratory

Collaborative Robotics System





Process Control System



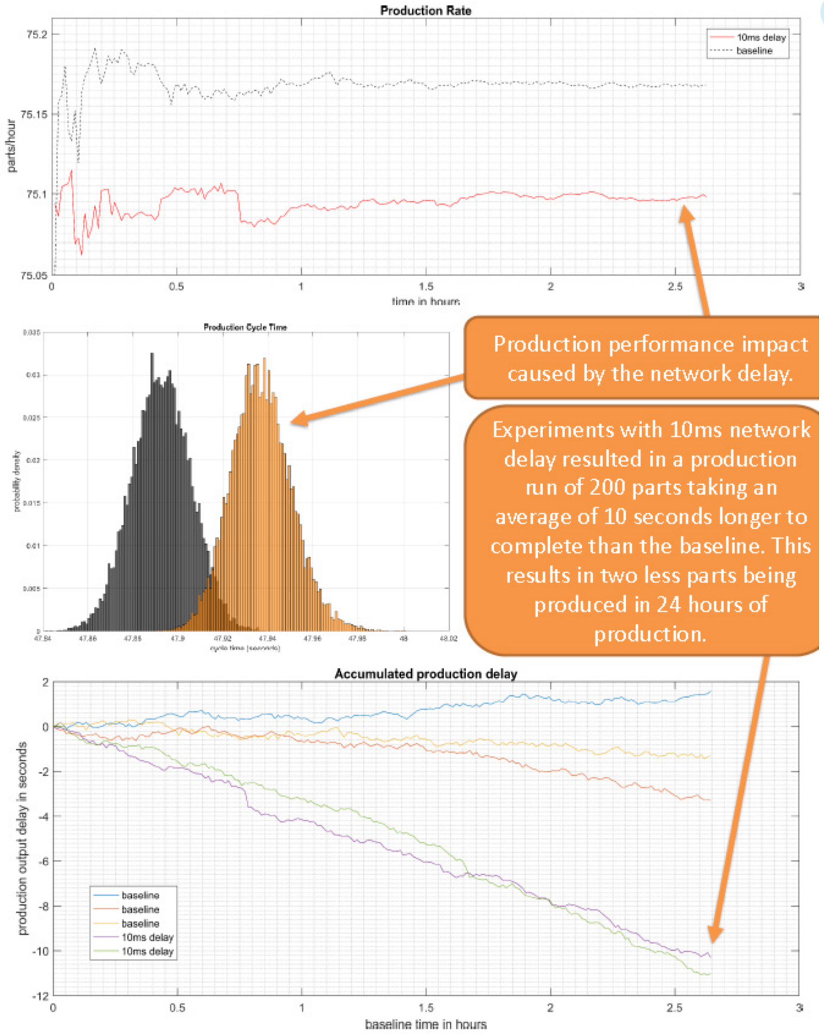
Measurement System

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

Example Measurements – Collaborative Robotics

Network	Production
Path Delay	Cycle Time
Inter-Packet Delay	Part Production Time
Round-Trip Time	Throughput Rate
Information Ratio	Effectiveness
Bit Rate	Utilization

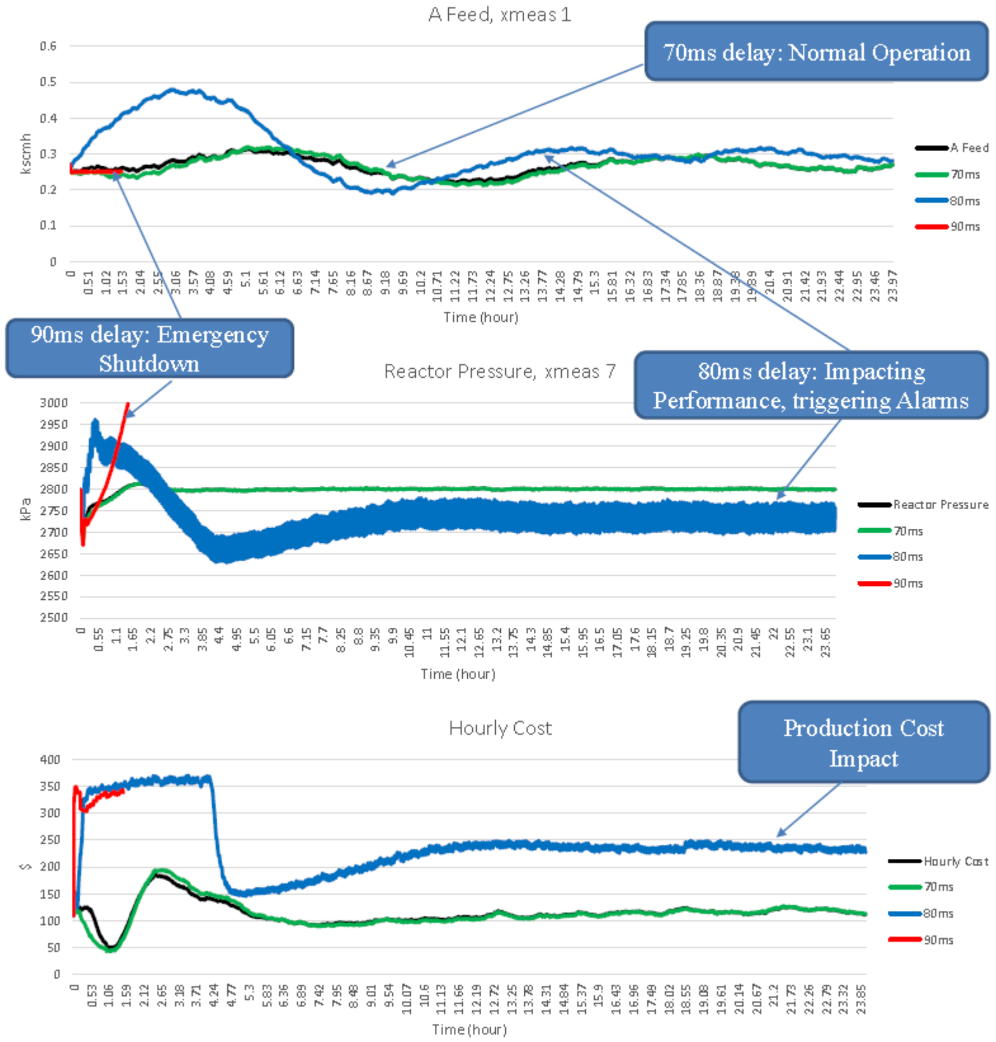
Computing Resources	Robot Performance
CPU Utilization	Actuation Latency
Memory Utilization	Pose Travel Time
Disk I/O	Position Accuracy
Interface Errors	



engineering laboratory

Example Measurements – Process Control

Network	Production
Path Delay	Output Yield
Round-Trip Time	Inputs Feed Rate
Packet Rate	Equipment Conditions
Packet Error Rate	Unplanned Stops
Packet Size Distribution	Unit Cost
Computing Resources	**Field Bus-DeviceNet(DN)**
CPU Utilization	DN Network Delay
Memory Utilization	DN Network Utilization
Disk I/O	DN Data Size
Process Execution Delay	
OPC DA Delay	



National Cybersecurity Center of Excellence (NCCoE) project

- NCCoE and the NIST Engineering Laboratory are collaborating to produce a series of Practice Guides demonstrating four cybersecurity capabilities for the manufacturing sector: behavioral anomaly detection, application whitelisting, malware detection and mitigation, and data integrity.
- NCCoE and EL are currently demonstrating behavioral anomaly detection and prevention mechanisms. The goal is to provide industry with detailed information to establish an anomaly detection and prevention capability in their own environments. By implementing behavioral anomaly detection tools, manufacturers are provided with a key security component that will aid in sustaining business operations, particularly those based on ICS.
- A behavioral anomaly detection for manufacturing Practice Guide, NIST SP 1800-10, will be developed from the research results. First draft of NIST SP 1800-10 is scheduled for May 2018.

https://nccoe.nist.gov/projects/use-cases/manufacturing

Thank You!

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