Industrial Control Systems Security Guide

Keith Stouffer, **Engineering Lab**

National Institute of Standards and Technology

NIST SP 800-82, Rev 2 and ICS Cybersecurity Testbed

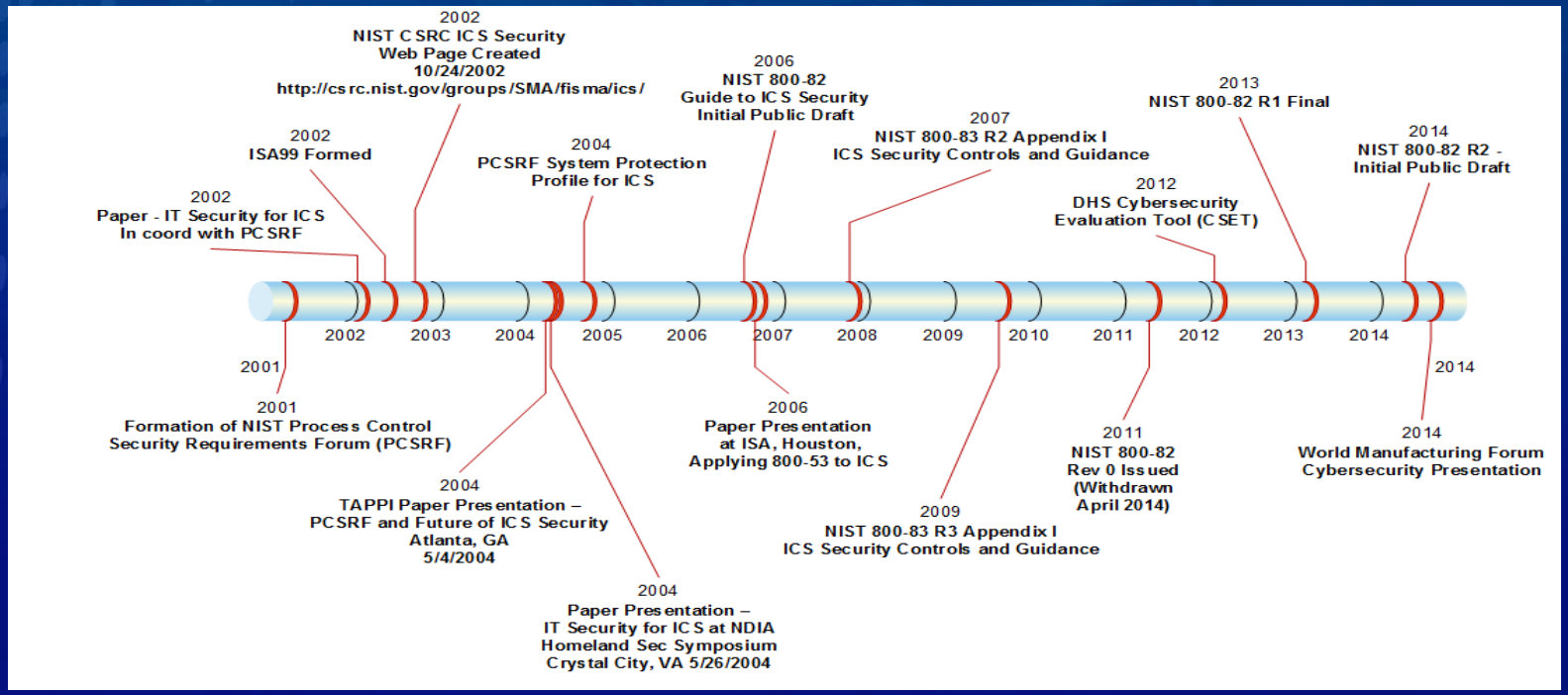
Keith Stouffer
Project Leader,
Cybersecurity for
Smart Manufacturing
Systems

Engineering Lab, NIST

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

Industrial Control System (ICS) Cybersecurity

- NIST has been a key player in the development of ICS cybersecurity standards and guidelines since 2000.



ICS 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 asses 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.

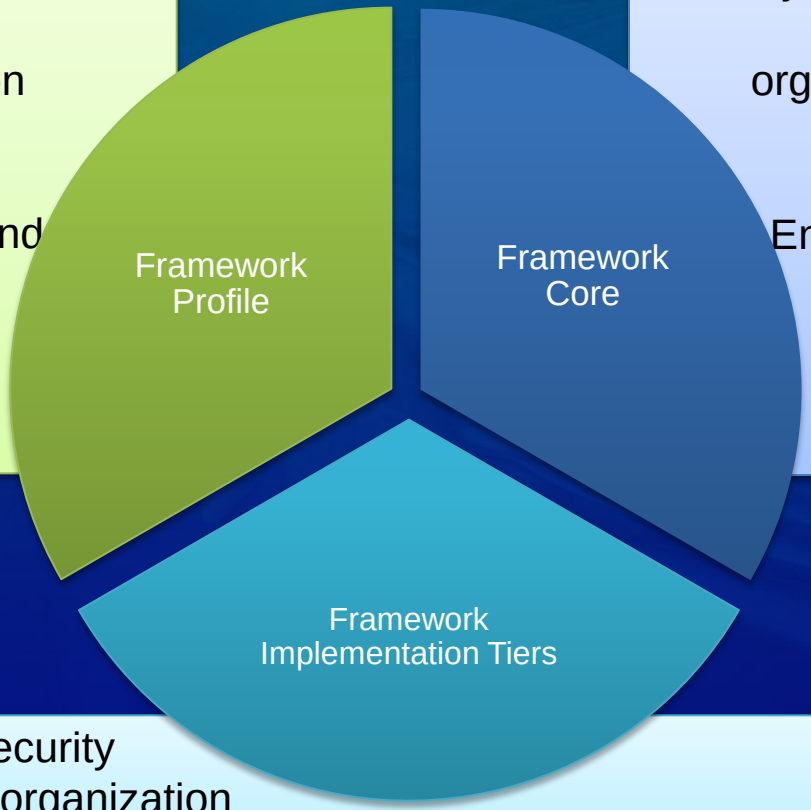
ICS Cybersecurity Research

- Implementation of the cybersecurity framework in various manufacturing scenarios including
  - Process Control
  - Collaborative Robotics
  - Additive Manufacturing
- Development of guidelines, methods, metrics and tools to enable manufacturers to implement the cybersecurity framework while addressing the demanding ICS performance, reliability, and safety requirements

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

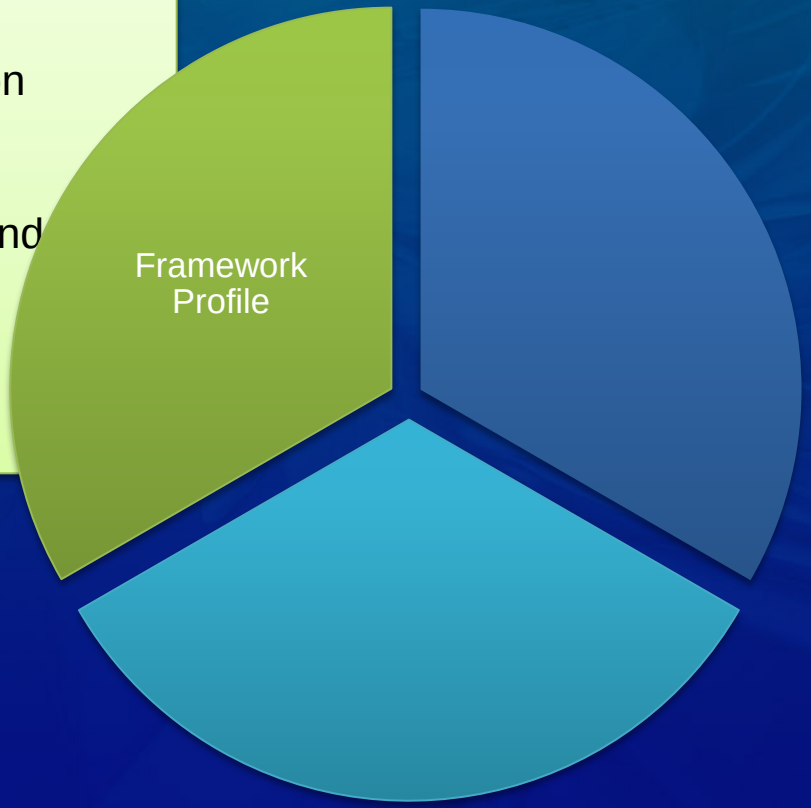
Enables communication of cyber risk across an organization

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

Framework Profiles

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

Supports prioritization and measurement while factoring in business needs



NIST ICS Cybersecurity 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 SP 800-82 and ISA/IEC 62443 standards
- 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 ICS Cybersecurity Testbed

- Reconfigurable nature of testbed will allow for researching various implementations for each ICS scenario

- Research outcomes will be used to provide guidance to industry on best practices for cost effectively implementing cybersecurity standards and guidelines without negatively impacting ICS performance

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
- Downloaded over 3,000,000 times since initial release in 2006 and is heavily referenced by the public and private industrial control community
- Revision 2 is currently in development

NIST SP 800-82

- Content
  - Overview of ICS
  - ICS Risk Management and Assessment
  - ICS Security Program Development and Deployment
  - ICS Security Architecture
  - Applying Security Controls to ICS
  - Appendixes
    - ICS Threats, Vulnerabilities, and Incidents
    - Activities in Industrial Control Systems Security
    - ICS Security Capabilities and Tools
    - ICS Overlay

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
- **Deploy security solution based on potential impact**
  - Not a one size fits all solution

ICS Overlay

- ICS overlay provides tailored NIST SP 800-53, Rev 4 security control baselines for Low, Moderate, and High impact ICS and adds supplementary guidance specific to ICS.
- 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).
- ICS overlay is included as Appendix G in NIST SP 800-82, Revision 2

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.

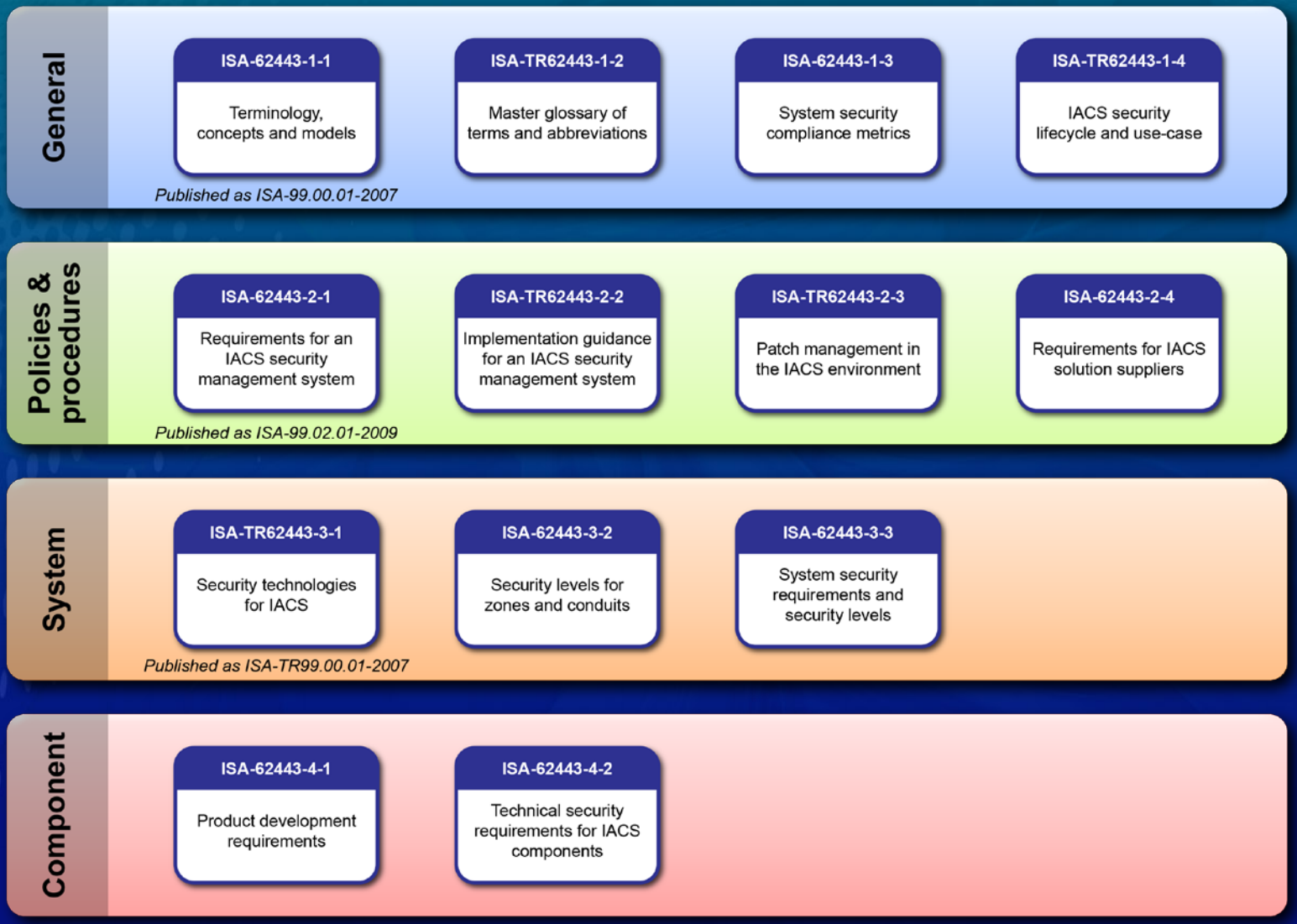
NIST SP 800-82, Rev 2 Schedule

- Initial public draft comment period on NIST SP 800-82, Rev 2 was May 15 – July 18, 2014
- Final public draft comment period is February 9 – March 9, 2015
  - Available on the NIST Computer Security Resource Center
  - http://csrc.nist.gov/publications/PubsSPs.html
- NIST SP 800-82, Rev 2 scheduled to be published May 2015

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

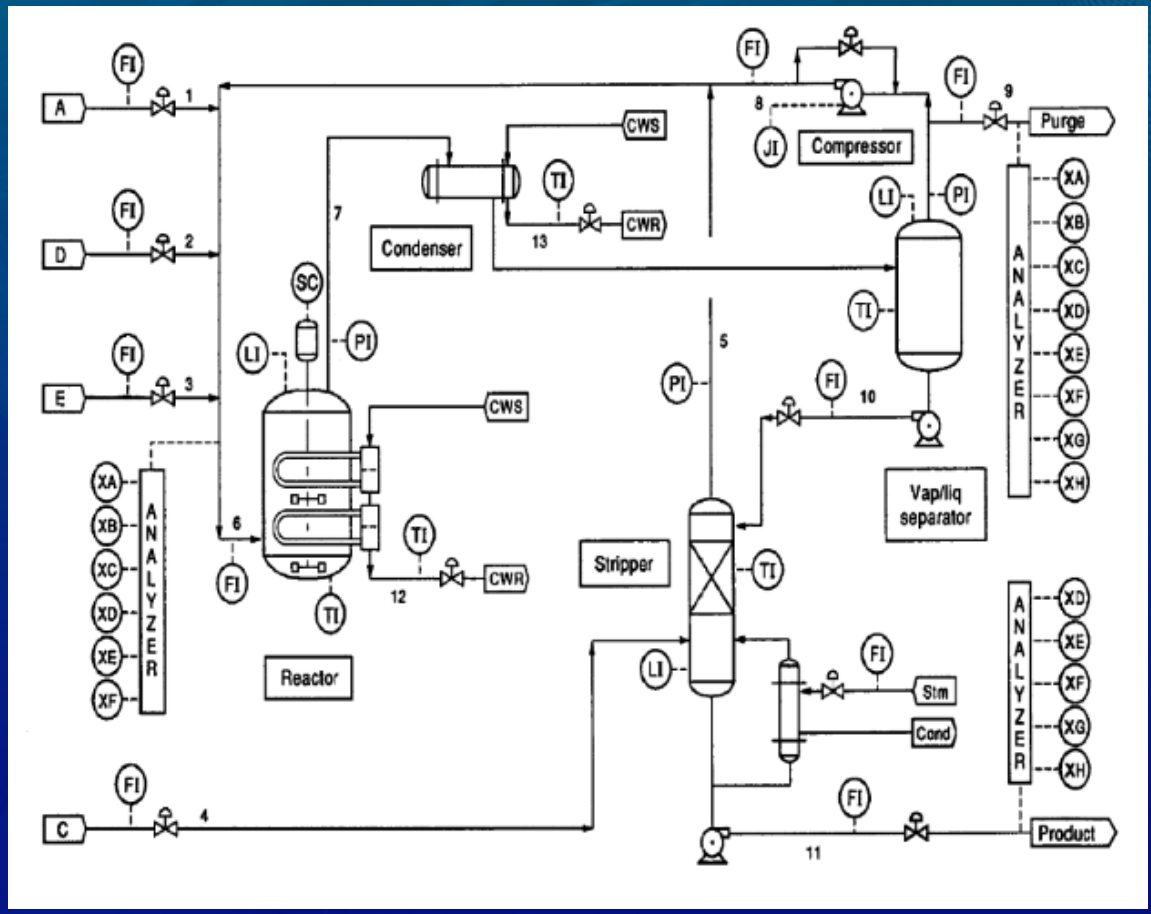


Testbed Scenarios

- 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

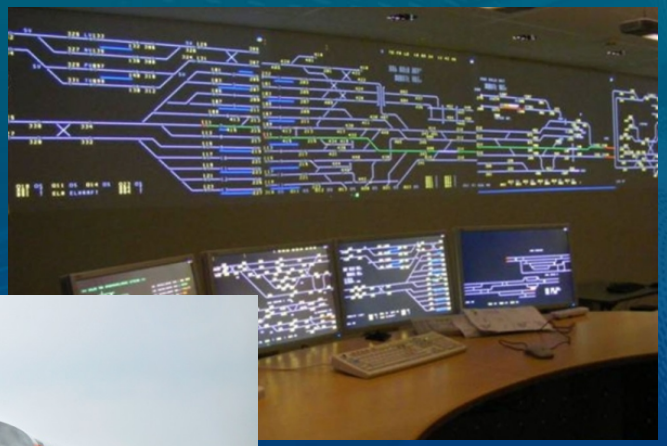


Dynamic Robotic Assembly

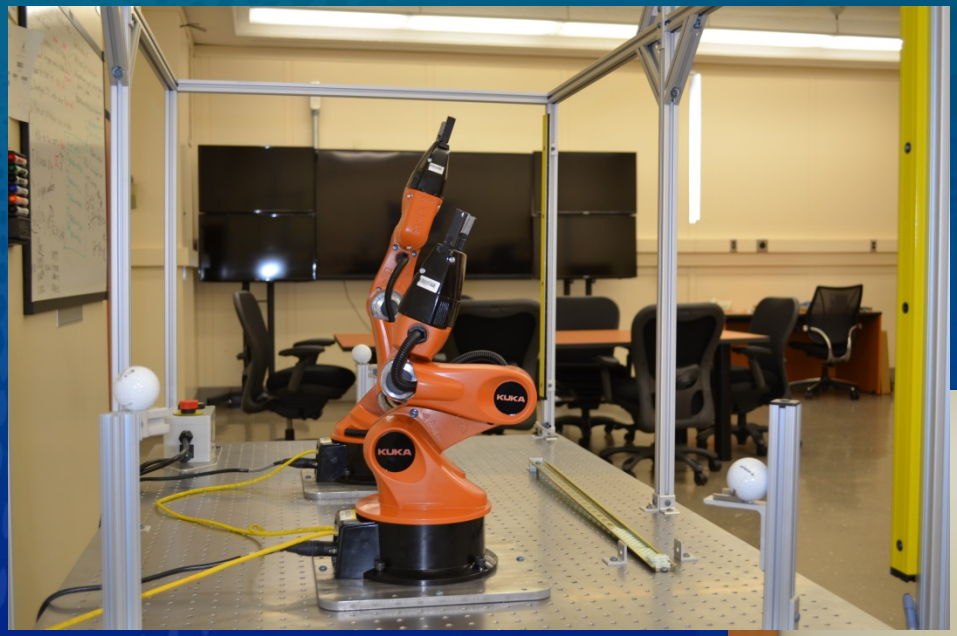
- Discrete process
- Cooperative robotics
- Dynamic Planning
- Integrated safety system
- Computer Vision
- Embedded control
- A variety of protocols including EtherCAT

Transportation

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



ICS Cybersecurity 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