National Cybersecurity Center of Excellence (NCCoE)

Manufacturing Sector Community of Interest

22 August 2017

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Agenda

- NIST / NCCoE Overview (Brief)
- NCCoE Manufacturing Sector Behavioral Anomaly Detection Project
- Guest Speaker: Robert M. Lee, Dragos Inc.
- Open Discussion / Comments / Questions

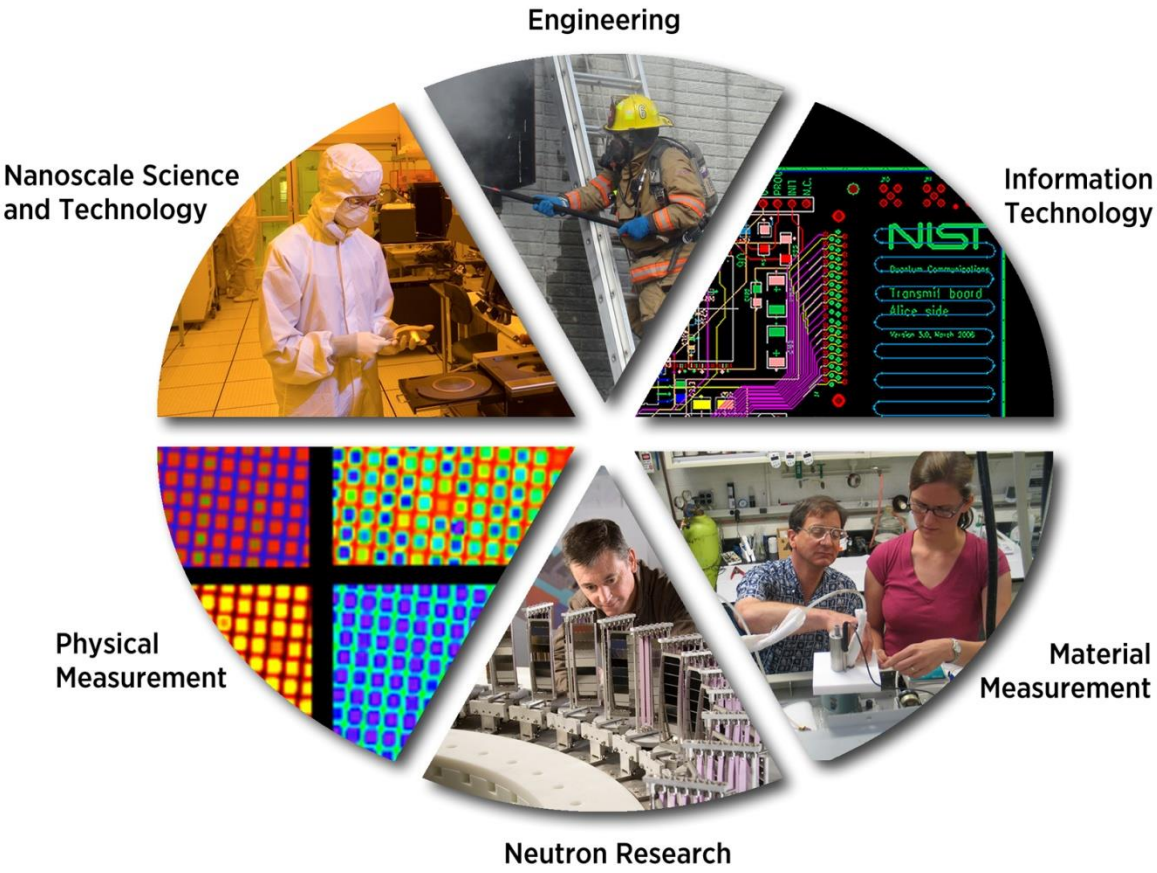
National Institute of Standards and Technology

NIST's work enables

- Science
- Technology innovation
- Trade
- Public benefit

NIST works with

- Industry
- Academia
- Government agencies
- Measurement labs
- Standards organizations



NIST's Laboratories

NIST Cybersecurity Portfolio

Areas of Focus	Some Major Activities
Cryptographic Technologies	Secure Hash Competition, Authentication, Key Management, Crypto Transitions, DNSSEC, E-Voting, Quantum Computing
Security Management and Assurance	Cybersecurity Framework for Critical Infrastructure, FISMA, Public Safety Network, Cyber-Physical System, Health IT, Smart Grid, Supply Chain, NICE, Outreach and Awareness
Secure Systems and Applications	Identity Management, Biometric Standards, Cloud Computing and Virtualization Technologies, Security Automation, Infrastructure Services and Protocols
Security Components and Mechanisms	Virtualization, Security Automation (SCAP), Trust Roots, Continuous Monitoring, USGv6
Security Test and Metrics Group	Crypto Validation Programs, CAVP, CMVP (FIPS 140), SCAP Validation, NVD
National Cybersecurity Center of Excellence	Work with business sectors to identify real-world cybersecurity opportunities and collaborate with IT vendors to develop commercially available solutions to accelerate the adoption of technology

NIST ITL

The NCCoE is part of the NIST Information Technology Laboratory and operates in close collaboration with the Computer Security Division. As a part of the NIST family, the center has access to a foundation of prodigious expertise, resources, relationships and experience.

PARTNERSHIPS

Established in 2012 through a partnership between NIST, the State of Maryland and Montgomery County, the NCCoE meets businesses' most pressing cybersecurity needs with reference designs that can be deployed rapidly.

NIST CYBERSECURITY THOUGHT LEADERSHIP

- Cryptography
- Identity management
- Key management
- Risk management
- Secure virtualization
- Software assurance
- Security automation
- Security for cloud and mobility
- Hardware roots of trust
- Vulnerability management
- Secure networking
- Usability and security

NCCOE CURRENT PROJECTS

Consumer/Retail

- Multifactor Authentication for e-Commerce

Energy

- Identity and Access Management
- Situational Awareness

Financial Services

- IT Asset Management
- Access Rights Management

Healthcare

- Electronic Health Records on Mobile Devices
- Infusion Pumps

Transportation: Maritime

- Cybersecurity Profile for Bulk Liquid Transfer

Public Safety/First Responder

- Mobile Single Sign-On
- Authentication for Law Enforcement Vehicle Systems

Manufacturing

- Behavioral Anomaly Detection

Mobile Device Security

- Mobile Device Security: Cloud & Hybrid Builds
- Mobile Threat Catalogue

Attribute Based Access Control

Data Integrity

Derived Personal Identity Verification (PIV)

DNS-based Secured Email

Manufacturing Behavioral Anomaly Detection Use Case :

- Final Project Description Published: 12/2016
- Finalized List of Collaborators: 06/30/2017
- https://nccoe.nist.gov/sites/default/files/library/project-descriptions/mf-ics-1-project-description-final.pdf
- Build Team Kickoff: 07/06/2015
- Projected Draft Practice Guide Release Date: 04/2018

MANUFACTURING BAD COLLABORATORS

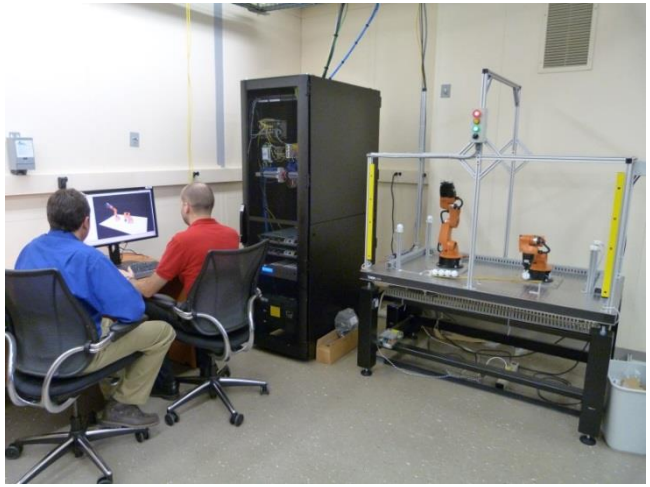
- **NCCoE Manufacturing BAD Collaborators:**
  - Cyber-X
  - GuardX
  - OSIsoft
  - SecureNok
  - Security Matters
  - Ultra-3eTi

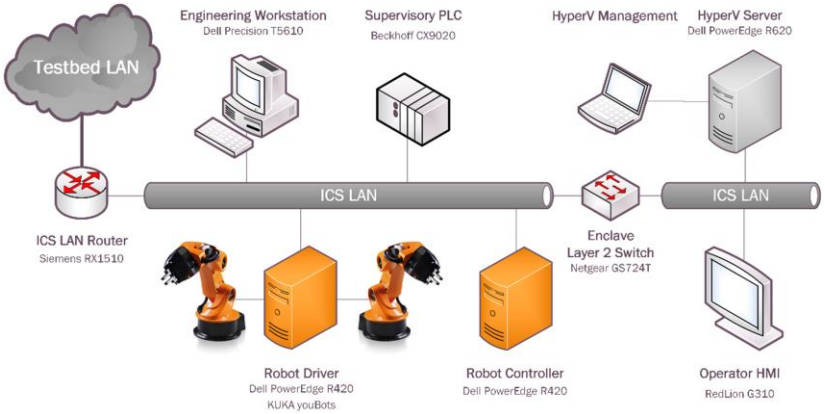
MANUFACTURING BAD: NIST EL & NCCOE

- Keith Stouffer NIST / EL - Principle Investigator
- Jim McCarthy NIST / NCCoE – Principle Investigator
- Chee Tang NIST / EL – Project Engineer
- Tim Zimmerman NIST / EL – Project Engineer
- Mike Powell NIST / NCCoE – Project Engineer

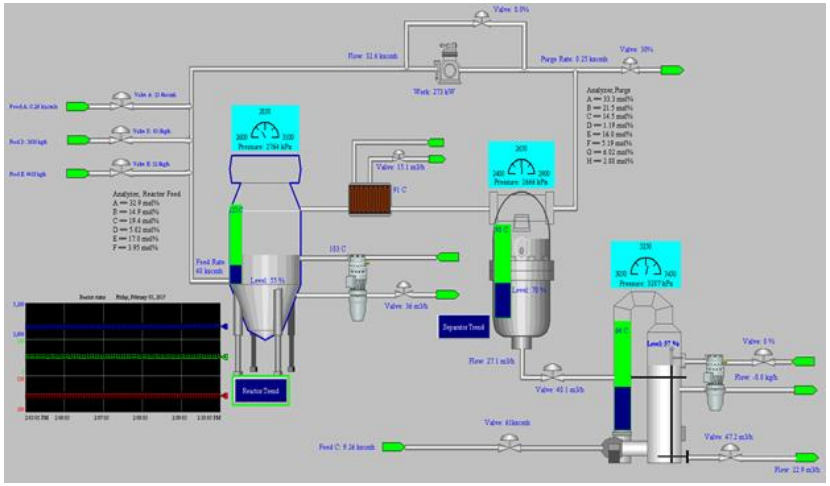
ARCHITECTURE

Collaborative Robotics System





Process Control System



HIGH LEVEL MILESTONES

- Build Architecture: 08/2017 – 09/2017
- Product Installations: 10/2017 – 11/2017
- Draft SP 1800-10 Assembly: 12/2017 – 01/2018
- Internal Review (includes BT): 02/2018 – 03/2018
- Release draft to public – 04/2018

GUEST SPEAKER

Robert M. Lee, CEO and Founder, Dragos Inc.

The Four Types of Threat Detection

EPC OPEN DISCUSSION

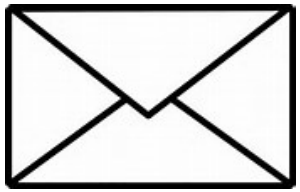
- Questions/comments

CONTACT US

301-975-0200

manufacturing_nccoe@nist.gov

9700 Great Seneca Hwy,
Rockville, MD 20850



100 Bureau Drive, Mail Stop 2002,
Gaithersburg, MD 20899

Thank You

STRATEGY

VISION

ADVANCE CYBERSECURITY

A secure cyber infrastructure that inspires technological innovation and fosters economic growth

MISSION

ACCELERATE ADOPTION OF SECURE TECHNOLOGIES

Collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

GOAL 1

PROVIDE PRACTICAL CYBERSECURITY

Help people secure their data and digital infrastructure by equipping them with practical ways to implement standards-based cybersecurity solutions that are modular, repeatable and scalable

GOAL 2

INCREASE RATE OF ADOPTION

Enable companies to rapidly deploy commercially available cybersecurity technologies by reducing technological, educational and economic barriers to adoption

GOAL 3

ACCELERATE INNOVATION

Empower innovators to creatively address businesses' most pressing cybersecurity challenges in a state-of-the-art, collaborative environment

NIST ITL

The NCCoE is part of the NIST Information Technology Laboratory and operates in close collaboration with the Computer Security Division. As a part of the NIST family, the center has access to a foundation of prodigious expertise, resources, relationships and experience.

PARTNERSHIPS

Established in 2012 through a partnership between NIST, the State of Maryland and Montgomery County, the NCCoE meets businesses' most pressing cybersecurity needs with reference designs that can be deployed rapidly.

NIST CYBERSECURITY THOUGHT LEADERSHIP

- Cryptography
- Identity management
- Key management
- Risk management
- Secure virtualization
- Software assurance
- Security automation
- Security for cloud and mobility
- Hardware roots of trust
- Vulnerability management
- Secure networking
- Usability and security

STAKEHOLDERS

SPONSORS

Advise and facilitate the center's strategy

- White House
- National Institute of Standards and Technology
- U.S. Department of Commerce
- U.S. Congress
- Montgomery County
- State of Maryland

TEAM MEMBERS

Collaborate to build real-world cybersecurity capabilities for end users

**Sponsored by NIST, the National Cybersecurity Federally Funded Research & Development Center (FFRDC) is operated by the MITRE Corporation*

- NCCoE
- National Cybersecurity FFRDC*
- Tech firms
- Industry
- Academia
- Government
- Project managers
- Project-specific collaborators
- National Cybersecurity Excellence Partners (NCEP)

END USERS

Work with center on use cases to address cybersecurity challenges

- Business sectors
- Individuals
- Academia
- Government
- Cybersecurity IT community
- Systems integrators

ENGAGEMENT & BUSINESS MODEL

DEFINE + ARTICULATE Describe the business problem	Define business problems and project descriptions, refine into a specific use case
ORGANIZE + ENGAGE Partner with innovators	Collaborate with partners from industry, government, academia and the IT community on reference design
IMPLEMENT + TEST Build a usable reference design	Practical, usable, repeatable reference design that addresses the business problem
TRANSFER + LEARN Guide users to stronger cybersecurity	Set of all material necessary to implement and easily adopt the reference design

BENEFITS

Cybersecurity solutions that are:

- based on standards and best practices
- usable, repeatable and can be adopted rapidly
- modular, end-to-end and commercially available
- developed using open and transparent processes
- matched to specific business needs and bridge technology gaps

The NCCoE seeks problems that are:

- Broadly applicable across much of a sector, or across sectors
- Addressable through one or more reference designs built in our labs
- Complex enough that our reference designs will need to be based on the combination of multiple commercially available technologies

Reference designs address:

- Sector-specific use cases that focus on a business-driven cybersecurity problem facing a particular sector (e.g., health care, energy, financial services)
- Technology-specific building blocks that cross sector boundaries (e.g., roots of trust in mobile devices, trusted cloud computing, software asset management, attribute based access control)