National Cybersecurity Center of Excellence

Michael Powell, Principal Investigator

Manufacturing Sector Community of Interest Call

Manufacturing_nccoe@nist.gov

June 27, 2019

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Agenda

- NCCoE Overview
- Introduction of Manufacturing Team
- Previous Manufacturing Project
- New Project: Detecting and Protecting Against Data Integrity Attacks in Industrial Control Systems Environments Project Description
- Questions/Comments

NCCoE Manufacturing Team: Contacts / Roles

Michael Powell	NIST/NCCoE – Principle Investigator	Michael.Powell@NIST.gov
Keith Stouffer	NIST – Principle Investigator	Keith.Stouffer@NIST.gov
Jim McCarthy	NIST/NCCoE – Senior Engineer	James.McCarthy@NIST.gov
CheeYee Tang	NIST – Project Engineer	Cheeyee.Tang@NIST.gov
Timothy Zimmerman	NIST – Project Engineer	Timothy.Zimmerman@NIST.gov
Titilayo Ogunyale	MITRE/NCCoE – Project Lead	TOgunyale@MITRE.org
Lura Danley	MITRE/NCCoE – Lead Social Scientist	LDanley@MITRE.org
Lauren Acierto	MITRE/NCCoE – Outreach & Engagement	LAcierto@MITRE.org

Mission

Accelerate adoption of secure technologies: collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

NCCoE Tenets

Standards-based

Apply relevant industry standards to each security implementation; demonstrate example solutions for new standards

Modular

Develop components that can be easily substituted with alternates that offer equivalent input-output specifications

Repeatable

Provide a detailed practice guide including a reference design, list of components, configuration files, relevant code, diagrams, tutorials, and instructions to enable system admins to recreate the example solution and achieve the same results

Commercially available

Work with the technology community to identify commercially available products that can be brought together in example solutions to address challenges identified by industry

Usable

Design blueprints that end users can easily and cost-effectively adopt and integrate into their businesses without disrupting day-to-day operations

Open and transparent

Use open and transparent processes to complete work; seek and incorporate public comments on NCCoE publications

Manufacturing Projects

Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection

- nccoe.nist.gov/nistir-8219

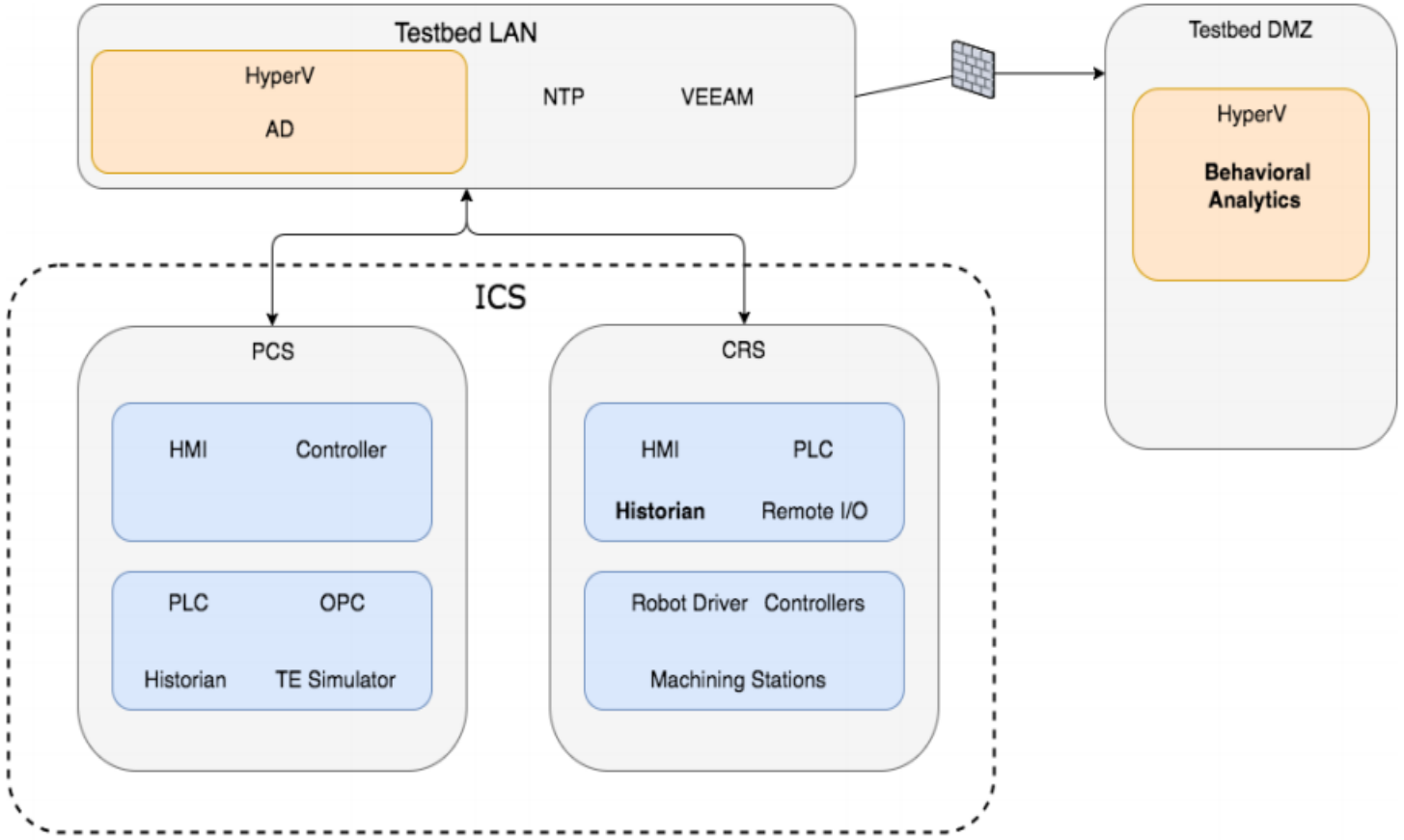
Detecting and Protecting Against Data Integrity Attacks in Industrial Control System Environments

- nccoe.nist.gov/ics-integrity

NISTIR 8219

Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection

- **Project focus:**
  - demonstrate behavioral anomaly detection techniques that businesses can implement and use to strengthen the cybersecurity of their manufacturing processes.
- **Three detection methods:**
  - network-based
  - agent-based
  - operational historian/sensor-based



Behavioral Anomaly Detection High Level Architecture

NISTIR 8219 Build Team

New Project: *Detecting and Protecting Against Data Integrity Attacks in Industrial Control Systems (ICS) Environments*

Project Focus:

- Provide a comprehensive approach that manufacturing organizations can use to address the challenge of protecting and detecting against data integrity attacks

Project Scope:

- Provide a proposed approach to prevent, mitigate, and detect threats from cyberattacks or insider threats within a manufacturing ICS environment
- Demonstrate how the commercially available technologies deployed in this build provide cybersecurity capabilities that manufacturing organizations can use to secure their operational technology (OT) systems

Cybersecurity Capabilities in New Project

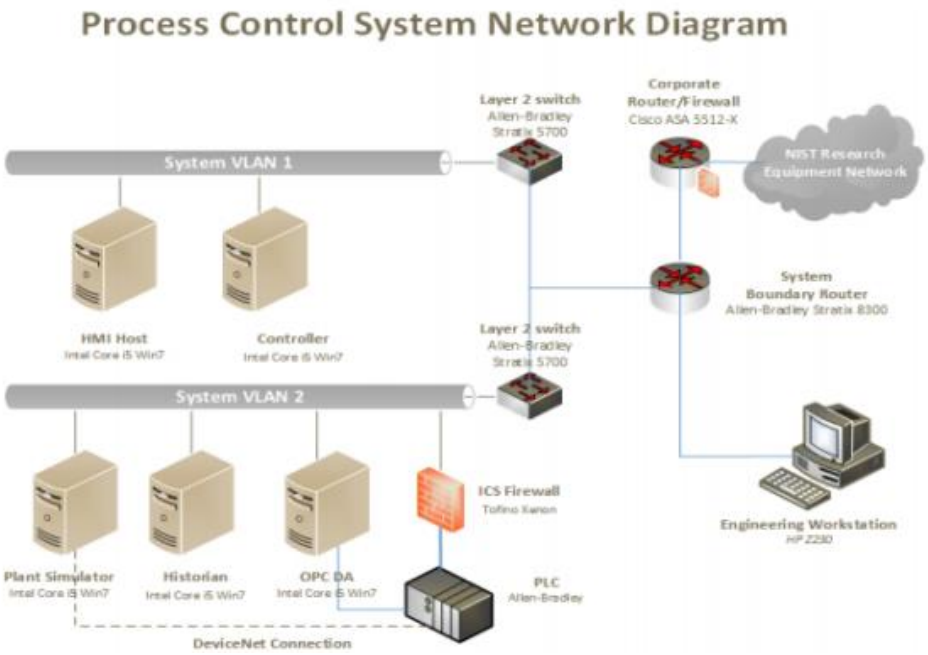
Detecting and Protecting Against Data Integrity Attacks in ICS Environments

- behavioral anomaly detection
- security incident and event monitoring
- ICS application whitelisting
- malware detection and mitigation
- change control management
- user authentication and authorization
- access control least privilege
- file integrity checking mechanisms

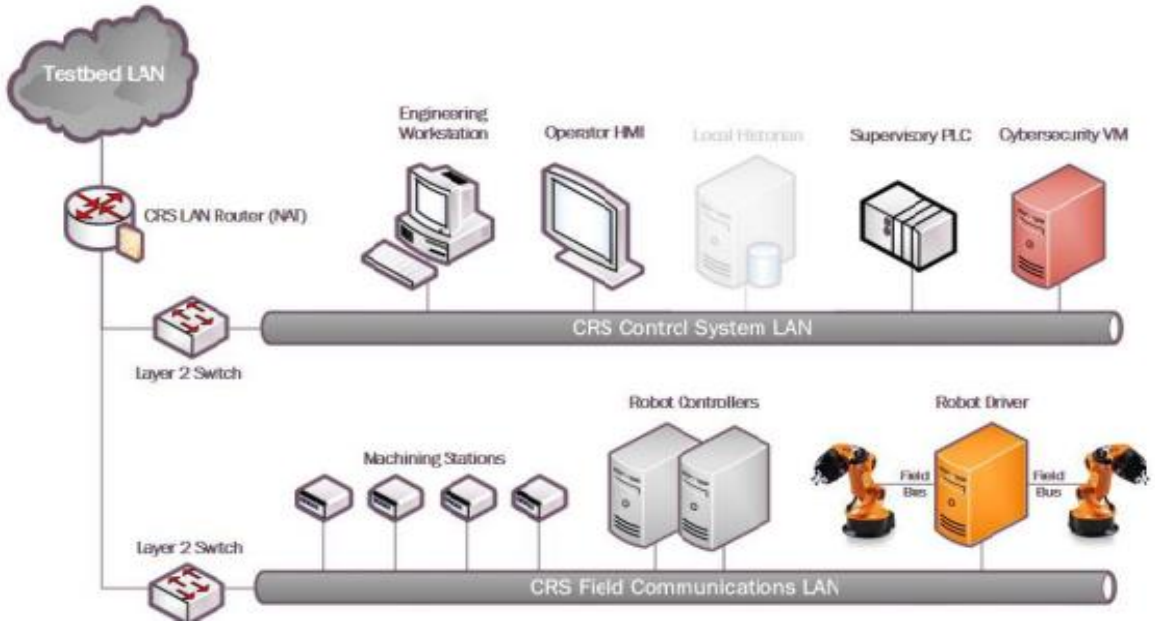
Multiple Capabilities in Two Manufacturing Demo Environments

Detecting and Protecting Against Data Integrity Attacks in ICS Environments

Process Control System Architecture



Robotics-Based Manufacturing Workcell Architecture



Project Execution Timeline

Detecting and Protecting Against Data Integrity Attacks in ICS Environments

DESCRIBE	FORM TEAM	DESIGN	BUILD PLAN	BUILD	DOCUMENT	OUTREACH
						
Publish the NCCoE project description	Form the team and complete the FRN, LOI, and CRADA	Design and engineer the architecture and usage scenarios taking into consideration resources	Develop the execution plan for building the demonstration based on the design	Compose, build the demonstration, and perform security functional tests	Develop the practice guide to publish as a public draft and final document	Present at public events and interact with community of interest
Q4 FY 2019	Q1 FY 2020	Q1 / Q2 FY 2020	Q1 / Q2 FY 2020	Q2 FY 2020 / Q3 FY 2020	Q3 / Q4 FY 2020	Q4 FY 2020

Next Steps

Detecting and Protecting Against Data Integrity Attacks in ICS Environments

Comment on the new Project Description:

- **Submit comments online or via email to manufacturing_nccoe@nist.gov.**
- **Public comment period ends July 25th**

Stay tuned for a call for collaborators via a Federal Register Notice (FRN):

- **Look out for email from us announcing FRN**
- **Check status on project webpage:**
- nccoe.nist.gov/ics-integrity

We Value Your Feedback

Do you:

- Have a success story from using one of our guides?
- Have comments/feedback regarding our guidance?
- Have an idea that you think the NCCoE should pursue?
- Know of an event where NCCoE should present?

Please engage with us: manufacturing_nccoe@nist.gov

Contact Us

Michael Powell, Principle Investigator

Manufacturing Sector Lead

Michael.Powell@NIST.gov

301-975-0310

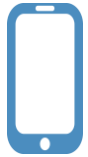
Titilayo Ogunyale

Project Lead

TOgunyale@MITRE.org

301-975-0219

http://nccoe.nist.gov



301-975-0200

nccoe@nist.gov