PROJECT DESCRIPTION

CAPABILITIES ASSESSMENT FOR SECURING MANUFACTURING INDUSTRIAL CONTROL SYSTEMS

Cybersecurity for Manufacturing

Keith Stouffer
NIST Engineering Laboratory

Jim McCarthy
NIST National Cybersecurity Center of Excellence (NCCoE)

DRAFT
November 7, 2016
Manufacturing_NCCoE@nist.gov

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) addresses businesses' most pressing cybersecurity problems with practical, standards-based solutions using commercially available technologies. The NCCoE collaborates with experts from industry, academia, and the government to build modular, open, end-to-end reference designs that are broadly applicable and repeatable. To learn more about the NCCoE, visit http://nccoe.nist.gov. To learn more about NIST, visit http://www.nist.gov.

This document describes a particular problem that is relevant across the manufacturing sector. NCCoE cybersecurity experts will address this challenge through collaboration with members of various manufacturing sectors and vendors of cybersecurity solutions. The resulting reference design will detail an approach that can be used by manufacturing sector organizations.

Abstract

Industrial Control Systems (ICS) monitor and control physical processes in many different industries and sectors. Cyber-attacks against ICS devices present a real threat to organizations that employ ICS to monitor and control manufacturing processes. The NIST Engineering Laboratory, in conjunction with the National Cybersecurity Center of Excellence, will produce a series of reference designs demonstrating four cybersecurity capabilities for manufacturing organizations. Each reference design will highlight an individual capability: Behavioral Anomaly Detection, ICS Application Whitelisting, Malware Detection and Mitigation, and ICS Data Integrity. This document is part one of a four-part series and addresses only behavioral anomaly detection capabilities.

With these capabilities in place, manufacturers will find it easier to detect anomalous conditions, control what programs and applications are executed in their operating environments, mitigate or vanquish malware attacks, and ensure the integrity of critical operational data.

For each of the four capabilities listed above, the NCCoE will map the security characteristics to the NIST Cyber Security Framework, which will provide standards-based security controls for manufacturers. In addition, the NCCoE will implement each of the capabilities in two distinct but related lab settings: a robotics-based manufacturing enclave, and a process control enclave, similar to what is being used by chemical manufacturing industries.

This project will result in a publicly available NIST Cybersecurity Practice Guide, a detailed implementation guide of the practical steps needed to implement the cybersecurity reference design that addresses this challenge.

Keywords

behavioral anomaly, control processes, Cyber Security Framework, CSF, industrial control system(s), ICS, manufacturing

Disclaimer

Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology or the National Cybersecurity Center of Excellence, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

Comments on NCCoE Documents

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at http://nccoe.nist.gov.

Comments on this publication may be submitted to: Manufacturing_NCCoE@nist.gov

Public comment period: *November 7, 2016 to December 7, 2016*

Table of Contents

1. Executive Summary

Purpose

This is the first of a four-part series designed to provide businesses with the information they need to establish an anomaly detection and prevention capability in their own environments. This project will be using commercially available software deployed on an established lab infrastructure. It will produce a mapping of security characteristics to the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) to establish a baseline that can be associated with specific security controls in prominent industry standards and guidance.

A cyber-attack directed at manufacturing infrastructure could result in detrimental consequences to both human life and property. Behavioral anomaly detection and prevention mechanisms can support a multi-faceted approach to counteracting cyber-attacks against Industrial Control Systems (ICS) devices that provide the functionality necessary to run manufacturing processes.

The goal of this project is to provide businesses with a cybersecurity reference design that can be implemented or that can inform improved cybersecurity in their manufacturing processes. We believe guarding against cyber-attacks will reduce costs for businesses that depend on these processes. Implementing behavioral anomaly detection tools provides a key security component in sustaining business operations, particularly those based on ICS. One of the ways to disrupt operations is to introduce anomalous data into a manufacturing process, whether deliberately or inadvertently. Although the reference design will focus on cybersecurity, our example solution may also produce residual benefit to manufacturers for detecting anomalous conditions not related to security.

Scope

This use case will focus on a single cybersecurity capability: behavioral anomaly detection. The NCCoE will deploy commercially available behavioral anomaly detection tools in two distinct but related manufacturing lab environments: a robotics enclave and a simulated chemical process enclave. The security characteristics of behavioral anomaly detection will be mapped to the CSF, which will point manufacturers to specific security controls found in prominent cybersecurity standards. This project will result in a NIST Cybersecurity Practice Guide, a detailed reference design document that will measure the performance of the behavioral anomaly detection tools and demonstrate how manufacturing companies can implement the capability in their own operational environments.

Assumptions/Challenges

The following assumptions and challenges will help shape the scope of the project and provide controlled parameters for the effort such that the focus is centered on delivering a successful solution based closely on the manufacturing operational environment.

Assumptions

- Manufacturing lab infrastructure is in place
- Numerous commercially available products exist in the market to demonstrate reference design

Challenges

- Findings may need to be extrapolated for large-scale manufacturing processes as the lab provides only a small-scale environment
- Lab environment consistency must be ensured as performance metrics of the products introduced are recorded and published

Background

The risk of cyber-attacks directed at ICS-based manufacturing infrastructures and processes is a great concern to companies who produce goods, particularly those made for public consumption. NIST recognizes this concern and is working with industry to solve these challenges through the implementation of cybersecurity technologies. In addition to this challenge, NIST provides the CSF for any manufacturing entity interested in enhancing the security of its infrastructure. The CSF is a valuable resource to those determining their next cybersecurity investment. This project will build an example of the implementation of a behavioral anomaly detection capability that manufacturers can adopt to achieve their cybersecurity goals.

2. SCENARIOS

Scenario 1: Robotics Enclave - Detecting anomalous conditions on a robotic-based manufacturing process

The robotics enclave contains a robotic assembly system in which industrial robots work cooperatively to move parts through a simulated manufacturing operation. The robots work according to a plan that changes dynamically based on process feedback. The robotic enclave includes two small, industrial grade robots and a supervisory Programmable Logic Controller (PLC) with safety processing. Additional information on the robotics enclave can be found at http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8089.pdf.

Scenario 2: Detecting anomalous conditions on a chemical manufacturing process

The process control enclave uses the Tennessee Eastman (TE) control problem as the continuous process model. The TE model is a well-known plant model used in control systems research, and the dynamics of the plant process are well understood. The process must be controlled—perturbations will drive the system into an unstable state. The inherent unstable open-loop operation of the TE process model presents a realworld scenario in which a cyber-attack could present a real risk to human and environmental safety, as well as economic viability. The process is complex and nonlinear, and has many degrees of freedom by which to control and disturb the dynamics of the process. Numerous simulations of the TE process have been developed with readily available reusable code. Additional information on the process control enclave can be found at http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8089.pdf.

3. High-Level Architectures

Robotics Enclave

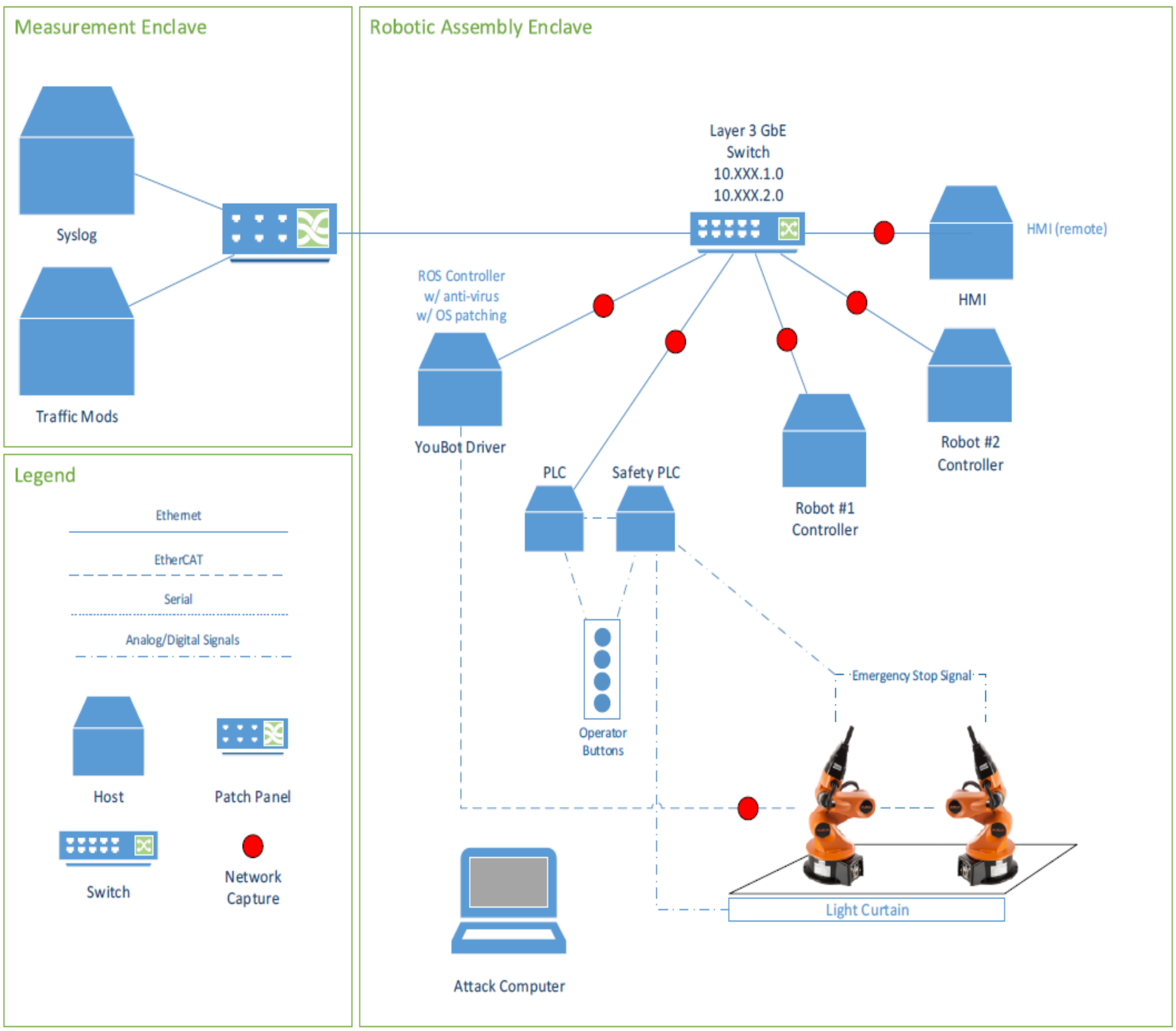

Figure 1. Robotics Enclave Architecture

Process Control Enclave

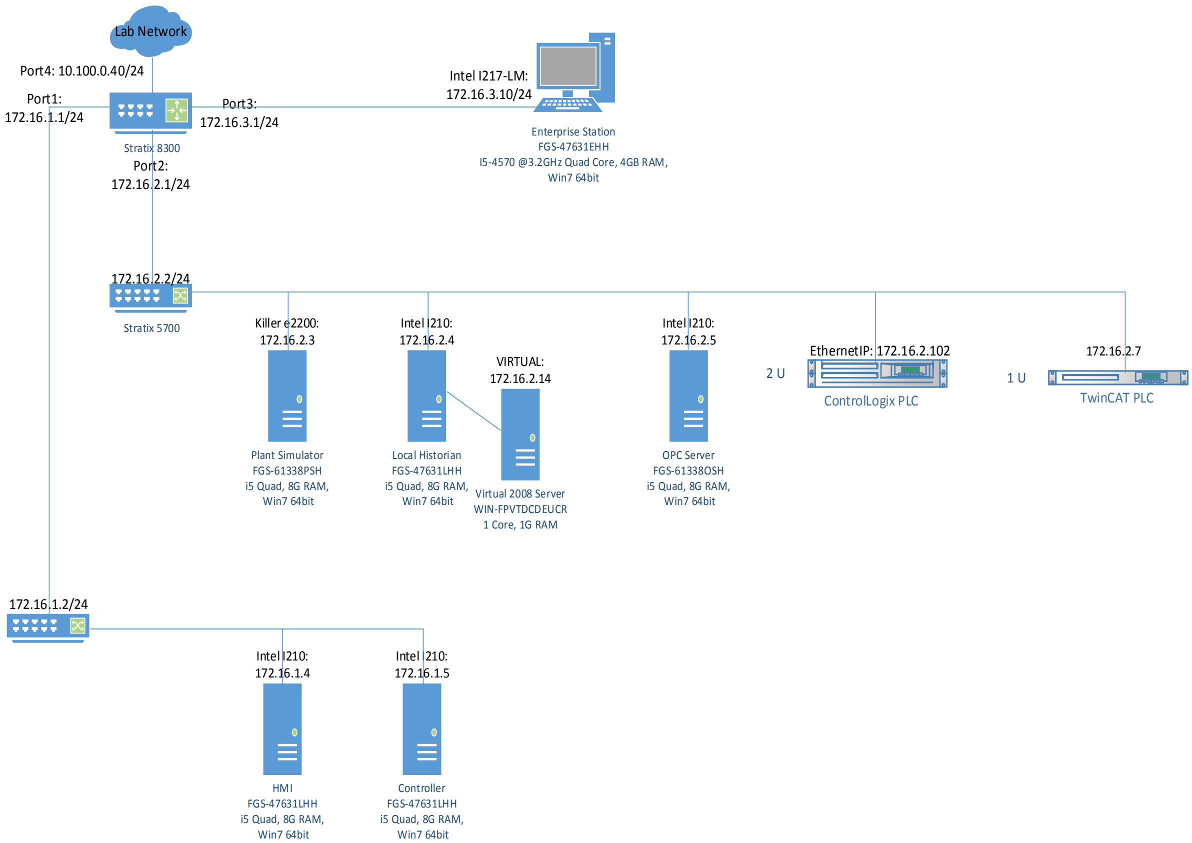

Figure 2. Process Control Enclave Architecture

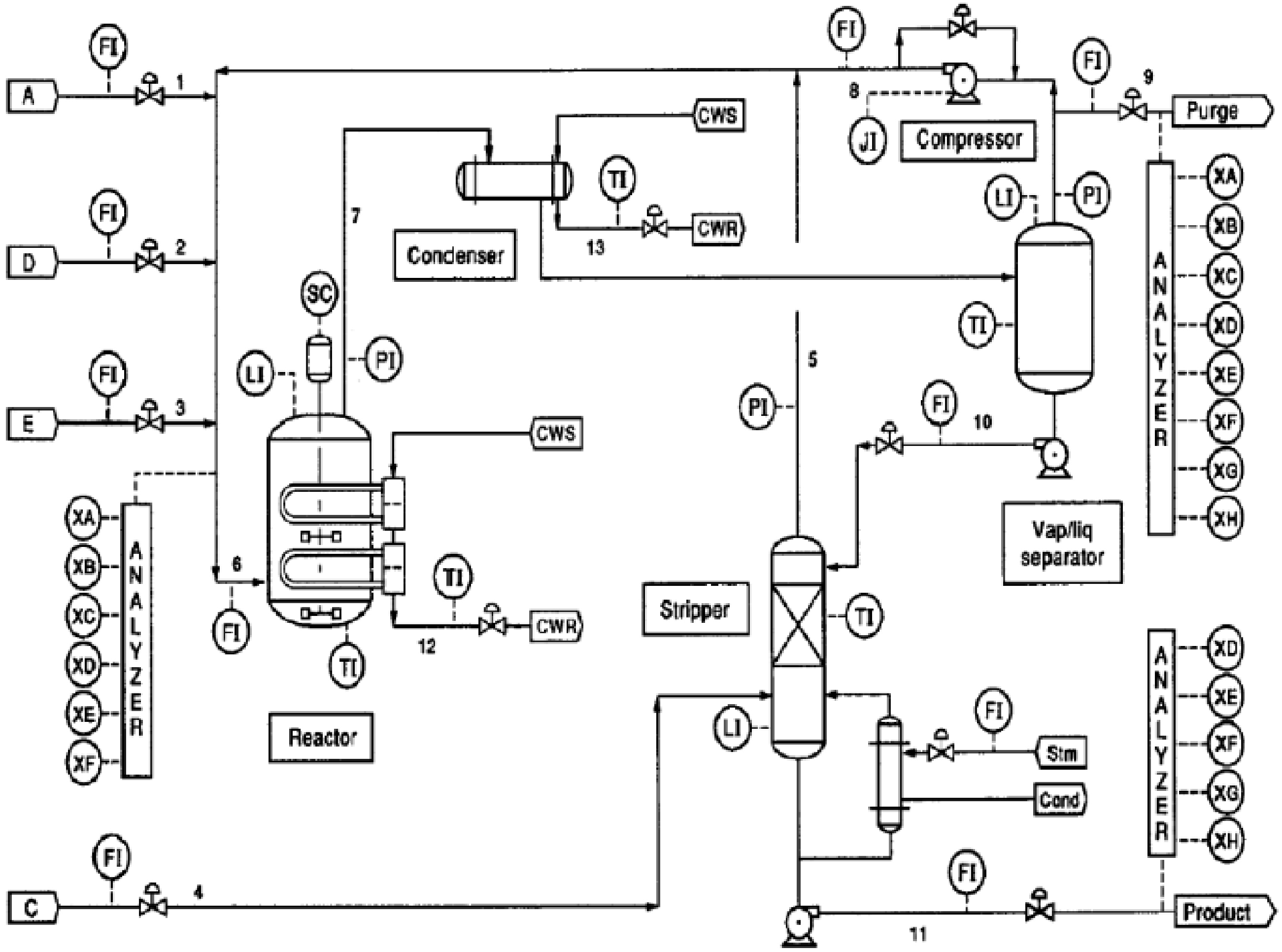

Figure 3. Tennessee Eastman process model

Component List

- ICS behavioral anomaly detection tools
- ICS application whitelisting tools
- ICS malware detection and mitigation tools
- ICS data integrity validation tools
- Human Machine Interfaces (HMIs)
- Programmable Logic Controllers (PLCs)
- Security Information and Event Management (SIEM) platform

Desired Requirements

- Detection of anomalous conditions
- Assurance of data integrity

- Detection of unauthorized applications
- Detection and mitigation of malware
- Detection of unauthorized data modification
- Process and/or device damage prevention
- Alerting/alarming capability

4. Relevant Standards and Guidance

- NIST SP 800-82, *Guide to Industrial Control Systems (ICS) Security*, *Revision 2*, May 2015. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
- *Cybersecurity Framework*, National Institute of Standards and Technology [Web site], http://www.nist.gov/cyberframework/ [accessed 2/25/14].
- Executive Order no. 13636, *Improving Critical Infrastructure Cybersecurity*, DCPD-201300091, February 12, 2013. http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf
- NISTIR 8089, *An Industrial Control System Cybersecurity Performance Testbed*, November 2015. http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8089.pdf
- Draft Cybersecurity Framework Manufacturing Profile, September, 2016. http://csrc.nist.gov/cyberframework/documents/csf-manufacturing-profile-draft.pdf

5. Security Control Map

Table 1. Cyber Security Framework Control Map

Function	Category	Subcategory	Manufacturing Profile	Reference
DETECT	DE.AE	DE.AE-1	**Low, Moderate and High** Ensure that a baseline of network operations and expected data flows for the manufacturing system is developed, documented, and maintained to detect events.	62443-2-1:2009 4.4.3.3 CM-2
		DE.AE-2	**Low** Review and analyze detected events within the manufacturing system to understand attack targets and methods.	62443-2-1:2009 4.3.4.5.6, 62443-3-3:2013 SR 2.8, 2.9 AU-6, IR-4
			Moderate and High Employ automated mechanisms where feasible to review and analyze detected events within the manufacturing system.	AU-6(1) IR-4(1)
		DE.AE-3	**Low and Moderate** Ensure that event data is compiled and correlated across the manufacturing system using various sources such as event reports, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.	62443-3-3:2013 SR 6.1 IR-5
			High Integrate analysis of events where feasible with the analysis of vulnerability scanning information; performance data; manufacturing system monitoring, and facility monitoring to further enhance the ability to identify inappropriate or unusual activity.	AU-6(5)(6) AU-12(1)
		DE.AE-4	**Low** Determine negative impacts to manufacturing operations, assets, and individuals resulting from detected events, and correlate with risk assessment outcomes.	RA-3
			Moderate Employ automated mechanisms to support impact analysis.	IR-4(1), SI-4(2)
			High Correlate detected event information and responses to achieve perspective on event impact across the organization.	IR-4(4)

Appendix A – References

R. Kuhn, Y. Lei and R. Kacker, "Practical Combinatorial Testing: Beyond Pairwise," *IT Professional*, vol. 10, no. 3, pp. 19-23, May-June 2008. http://dx.doi.org/10.1109/MITP.2008.54.