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

March 2017
Manufacturing_NCCoE@nist.gov

This revision incorporates comments from the public.

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries or broad, cross-sector technology challenges. Working with technology partners—from Fortune 50 market leaders to smaller companies specializing in IT security—the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology. Information is available at: https://nccoe.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 example solution 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 (EL), in conjunction with the National Cybersecurity Center of Excellence, will produce a series of example solutions demonstrating four cybersecurity capabilities for manufacturing organizations. Each example solution 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 may find it easier to detect anomalous conditions, control what programs and applications are executed in their operating environments, mitigate malware attacks, and ensure the integrity of critical operational data.

For each of the four capabilities listed above, the NIST EL and the NCCoE will map the security characteristics to the NIST Cybersecurity Framework (CSF), which will provide standards-based security controls for manufacturers. In addition, the EL and 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 that resembles 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 example solution that addresses this challenge.

KEYWORDS

behavioral anomaly, control processes, Cybersecurity 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.

All comments are subject to release under the Freedom of Information Act (FOIA).

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 hardware and software deployed on an established lab infrastructure. It will produce a mapping of security characteristics to the Cybersecurity Framework (CSF) to establish a reference that can be associated with specific security controls in prominent industry standards and guidance.

This project will focus on behavioral anomaly detection, which is defined here as a mechanism that establishes a baseline system model, profiles system behavior, and continuously monitors the system to detect and alert deviations in system behavior that are uncommon, peculiar, irregular, or abnormal. 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 a cybersecurity example solution that businesses can implement or use to strengthen cybersecurity in their manufacturing processes. Implementing behavioral anomaly detection tools can provide 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 example solution will focus on cybersecurity, it may also produce residual benefit to manufacturers in 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 guide that will demonstrate how manufacturing companies can implement behavioral anomaly detection tools without negatively impacting the performance of their operational environments.

Assumptions/Challenges

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

Assumptions

- A manufacturing lab infrastructure is in place.
- Numerous commercially available behavioral anomaly detection products exist in the market to demonstrate the example solution.

Challenges

- The lab environment is on a smaller scale than many commercial manufacturing environments and may not contain all the devices that would typically be found in a real-world setting (see Robotics and Process Control Enclave diagrams in Section 3).
- The lab environment emulates a real-world setting. However, it is important to note the lab environment we are using likely provides a limited representation of real-world manufacturing environments, especially in regards to the number of devices being used (see Robotics and Process Control Enclave diagrams in Section 3).

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 development of reference designs and practical application 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 implementation of a behavioral anomaly detection capability that manufacturers can adopt to achieve their cybersecurity goals.

2. SCENARIOS

NIST conducted a two-day Road Mapping Workshop on Measurement of Security Technology Performance Impacts for Industrial Control Systems, held at NIST, on December 4-5, 2013. The participants represented a balanced cross-section of industrial control system (ICS) stakeholder groups, including manufacturers, technology providers, solution providers, university researchers, and government agencies. The Workshop results served as a foundation for the manufacturing scenarios researched in the lab. The Workshop report can be found at https://www.nist.gov/sites/default/files/documents/el/isd/cs/NIST_ICS-Workshop-FinalReport.pdf.

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

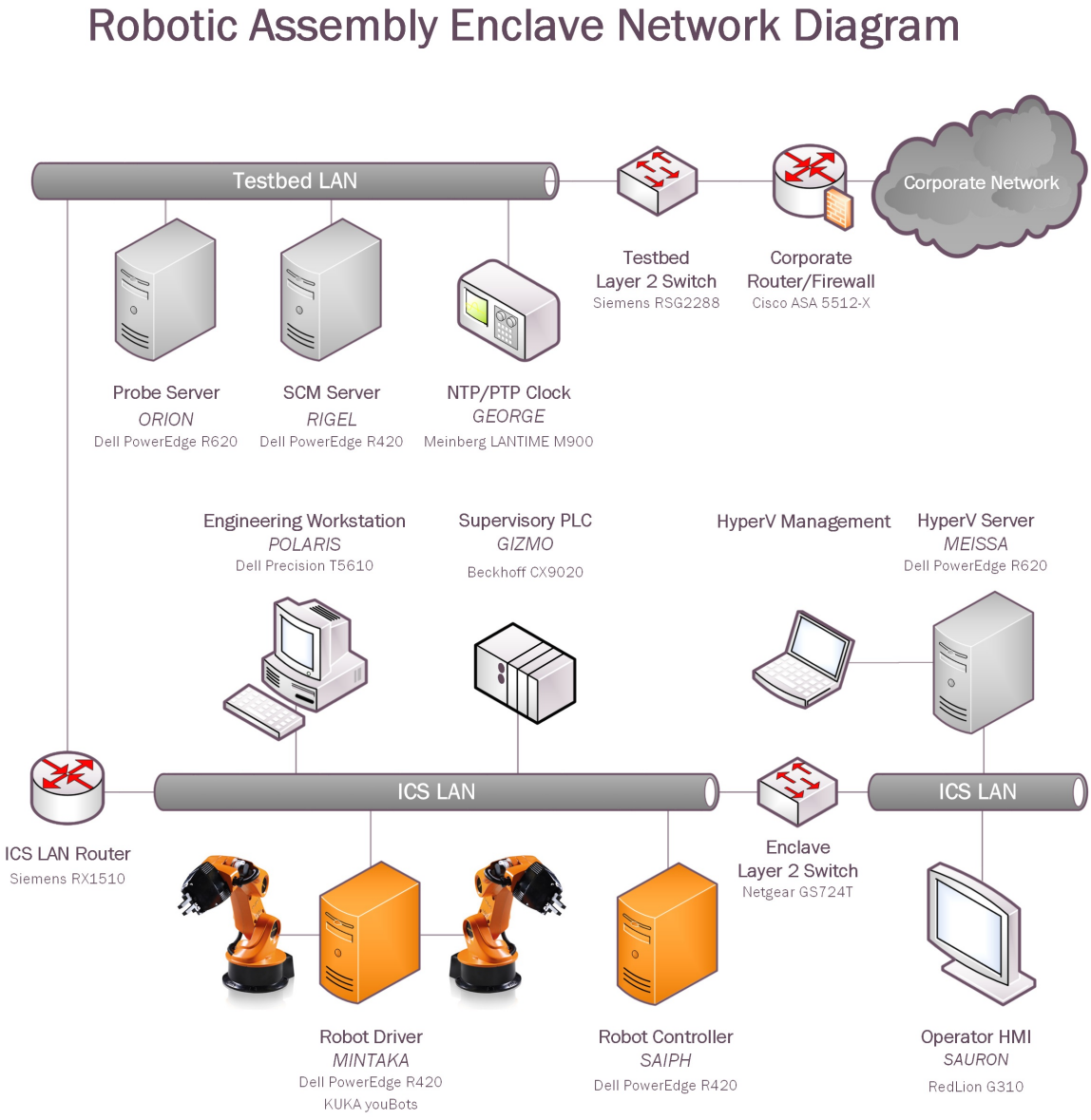
The robotics enclave contains a robotic assembly system in which industrial robots work cooperatively to move parts through a simulated manufacturing operation. The robots work according to a plan that changes dynamically based on process feedback. The robotics enclave includes two small, industrial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

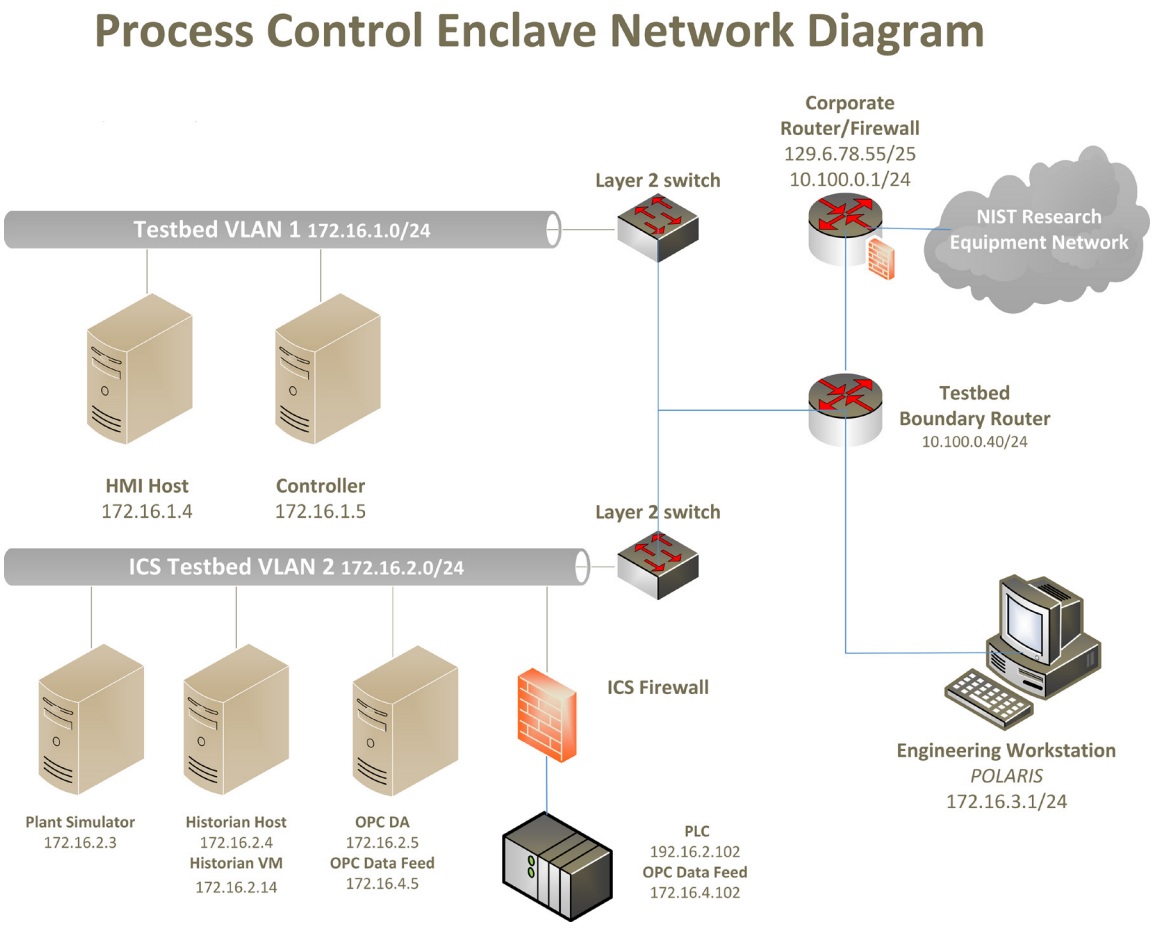
3. EXISTING HIGH-LEVEL LAB ARCHITECTURES

Robotics Enclave

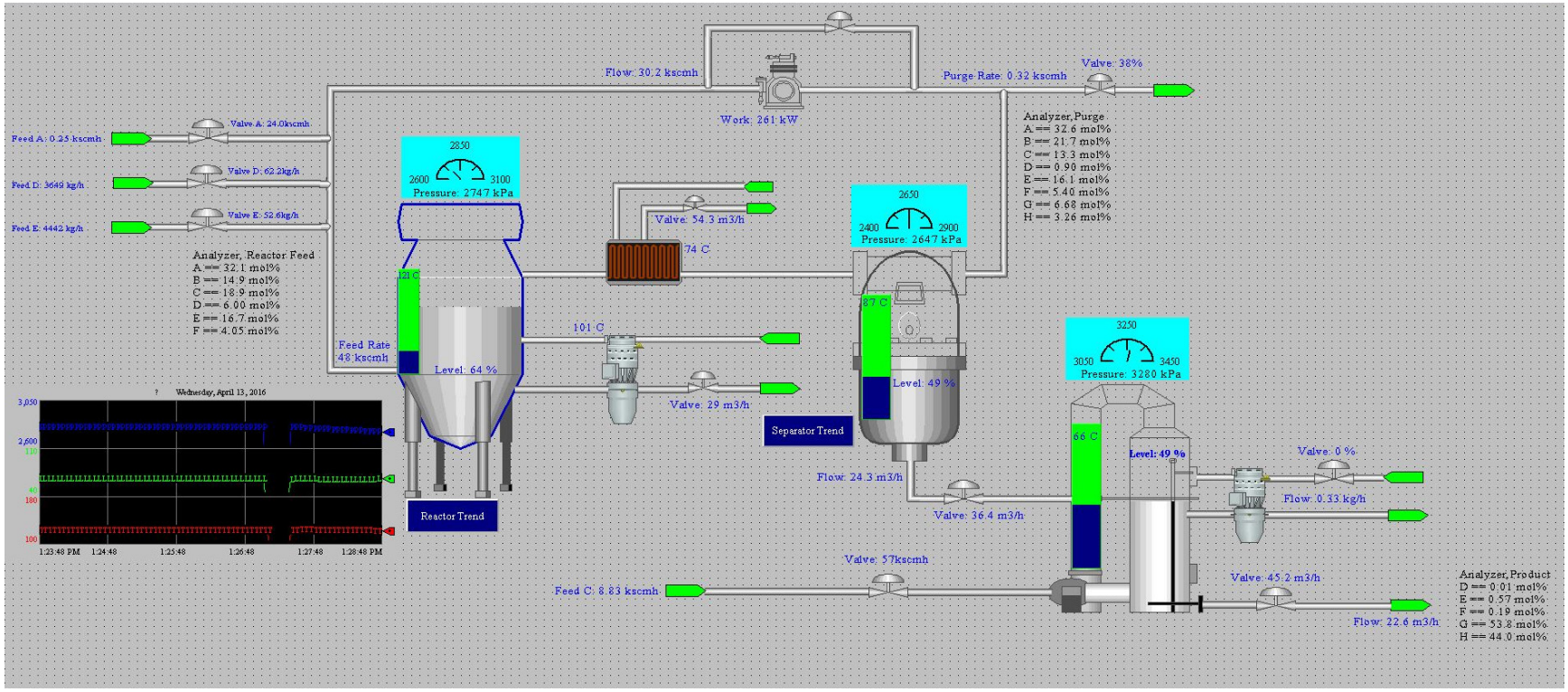


Additional information on the robotics enclave can be found at http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8089.pdf.

Process Control Enclave



Tennessee Eastman Process Model



Additional information on the process control enclave and the Tennessee Eastman process can be found at http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8089.pdf.

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
- SIEM-based alerting/alarming capability

4. SECURITY CONTROL MAP

Cybersecurity Framework Manufacturing Profile Control Map

Function	Category	Subcategory	Manufacturing Profile	Reference
DETECT	DE.AE	DE.AE-1	**Low, Moderate and High**	62443-2-1:2009 4.4.3.3
			Ensure that a baseline of network operations and expected data flows for the manufacturing system is developed, documented, and maintained to detect events.	CM-2
		DE.AE-2	**Low**	62443-2-1:2009 4.3.4.5.6, 62443-3-3:2013 SR 2.8, 2.9
			Review and analyze detected events within the manufacturing system to understand attack targets and methods.	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**	62443-3-3:2013 SR 6.1
			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.	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.

K. Stouffer, V. Pilliteri, S. Lightman, M. Abrams, and A. Hahn, *Guide to Industrial Control Systems (ICS) Security*, *Revision 2*, NIST SP 800-82 rev2, May 2015. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Cybersecurity Framework, National Institute of Standards and Technology, 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

R. Candell, T. Zimmerman, and K. Stouffer, *An Industrial Control System Cybersecurity Performance Testbed*, NISTIR 8089, November 2015. http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8089.pdf

Cybersecurity Framework Manufacturing Profile, Draft, National Institute of Standards and Technology, September, 2016. http://csrc.nist.gov/cyberframework/documents/csf-manufacturing-profile-draft.pdf