PROJECT DESCRIPTION

PROTECTING INFORMATION AND SYSTEM INTEGRITY IN INDUSTRIAL CONTROL SYSTEM ENVIRONMENTS

Cybersecurity for the Manufacturing Sector

Keith Stouffer
Cheeyee Tang
Timothy Zimmerman
Engineering Laboratory
National Institute of Standards and Technology

Michael Powell
Jim McCarthy
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Titilayo Ogunyale
Lauren Acierto
Lura Danley
The MITRE Corporation

February 2020

Manufacturing_NCCoE@nist.gov

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. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices by using commercially available technology. To learn more about the NCCoE, visit http://www.nccoe.nist.gov. To learn more about NIST, visit http://www.nist.gov.

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

Acronyms used in figures can be found in Appendix B, Acronyms and Abbreviations.

ABSTRACT

Manufacturing organizations that rely on industrial control systems (ICS) to monitor and control physical processes that produce goods for public consumption are facing an increasing number of cyber attacks. The U.S. Department of Homeland Security reports that the manufacturing industry is the second most targeted industry, based on the number of reported cyber attacks [1]. Given how critical ICS are to operations, cyber attacks against ICS devices present a real threat to safety and production, which can result in damaging economic impact to a manufacturing organization.

The NCCoE part of NIST's Information Technology Laboratory, in conjunction with the NIST Engineering Laboratory (EL) and industry collaborators, will highlight how an organization can take a comprehensive approach to securing ICS within the manufacturing sector by leveraging the following cybersecurity capabilities: 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, and file-integrity-checking mechanisms.

The goal of this project is to demonstrate an example solution that protects the integrity of data from destructive malware, insider threats, and unauthorized software within manufacturing environments that rely on ICS. The EL and the NCCoE will map the security characteristics to the NIST Cybersecurity Framework; the National Initiative for Cybersecurity Education Framework; and NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, and will provide standards-based security controls for manufacturers. Additionally, NIST will implement each of the listed capabilities in two distinct but related existing lab settings: a discrete-based manufacturing workcell and a process control system that resembles what is being used by chemical manufacturing industries. This project will result in a freely available NIST Cybersecurity Practice Guide.

KEYWORDS

access control least privilege; application whitelisting; behavioral anomaly detection; change control management; file integrity; industrial control systems; malware detection and mitigation; manufacturing; security incident and event monitoring; unauthorized software

DISCLAIMER

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 EXECUTIVE SUMMARY

Purpose

Industrial control systems (ICS) in manufacturing environments are increasingly subject to cyber attacks and insider threats. To enhance system security, manufacturing organizations must be able to detect and protect against system and information-integrity attacks. Such threats to system and information integrity could compromise critical manufacturing programs, decrease productivity, and negatively impact safety and business operations. This project will provide a comprehensive approach that manufacturing organizations can use to address the challenge of detecting and protecting against system and information-integrity attacks, which leverages the following cybersecurity capabilities: 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, and file-integrity-checking mechanisms.

Publication of this project description is the beginning of a process that will identify project collaborators as well as standards-based, commercially available, and open-source hardware and software components. These products will be integrated and implemented in existing National Institute of Standards and Technology (NIST) laboratory environments, to build open, standards-based, modular, end-to-end reference designs that will address the security challenges of system and information-integrity attacks within the manufacturing sector. The approach may include architectural definition, logical design, build development, security analysis, test and evaluation, security control mapping, and future build considerations. This project will result in a publicly available NIST Cybersecurity Practice Guide, a detailed implementation guide of the practical steps needed to implement a cybersecurity reference design that addresses this challenge.

Scope

These are the objectives of this project:

- provide a proposed approach to prevent, detect, and mitigate threats from cyber attacks or insider threats within discrete and process manufacturing environments
- provide a proposed approach to detect misconfigurations and device faults
- 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

Specifically, the results of this project will answer the following questions:

- What capabilities are needed to prevent unwanted modifications within ICS that use functionality verification, system and information-integrity checking, intrusion detection, malicious code detection, and security alert and advisory controls requirements?
- What protections are needed for detecting and controlling modifications to hardware, firmware, and software, and what documentation is needed to ensure ICS are protected against improper modifications prior to, during, and after system implementation?
- What processes are needed to verify the identity of a user, process, or device when using specific credentials?

- What mechanisms can be used for protecting both system and data transmission components?
- How can baselining of typical communication patterns assist in monitoring industrial controllers?

This project will address:

- detection/prevention of unauthorized software installation
- security incident and event monitoring to identify, monitor, record, and analyze security events and incidents within a real-time OT environment
- whitelisting to protect computers and ICS networks from potentially harmful applications
- change control management tools to determine if improper changes are made to a product or system
- a user authentication and authorization solution to detect authenticated but unauthorized use of the system
- file-integrity monitoring to validate the integrity of operating systems and application software files
- behavioral and anomaly detection tools to continuously monitor the network for unusual events or trends
- malware detection and mitigation of any software designed to damage a computer, server, or computer network

Assumptions

A manufacturing lab infrastructure is in place at NIST that represents discrete (collaborative robotics system shown in Figure 4-2) and process (continuous chemical process system shown in Figure 5-1) manufacturing environments. Numerous commercially available off-the-shelf technologies exist in the market to demonstrate the example solutions.

Challenges

While the lab environment simulates a real-world setting, it is important to note that the lab is on a smaller scale than many commercial manufacturing environments. Thus it likely provides a limited representation of real-world manufacturing environments, especially regarding the number of devices being used.

Background

As stated in NIST Special Publication (SP) 800-82 Revision 2*, Guide to Industrial Control Systems (ICS) Security*, ICS are vital to operation of the United States' critical infrastructures, which are often highly interconnected and mutually dependent systems. While federal agencies also operate many ICS, approximately 90 percent of the nation's critical infrastructures are privately owned and operated. As ICS increasingly adopt information technology (IT) to promote corporate business systems' connectivity and remote access capabilities, the accompanying integration provides significantly less isolation for ICS from the outside world. While security controls have been designed to deal with security issues in typical IT systems, special precautions must be taken when introducing these same approaches in ICS environments. In some cases, new security techniques tailored to the specific ICS environment are needed.

The National Cybersecurity Center of Excellence (NCCoE) recognizes this concern and is working with industry through consortia under Cooperative Research and Development Agreements

with technology partners from Fortune 50 market leaders to smaller companies specializing in IT security. The aim is to solve these challenges by developing reference designs and practical applications of cybersecurity technologies. This project will build upon NIST Interagency or Internal Report 8219, *Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection,* by identifying additional tools to improve ICS security.

2 SCENARIOS

NIST conducted a two-day Roadmap for Measurement of Security Technology Impacts for Industrial Control Systems workshop December 4–5, 2013. The participants represented a balanced cross-section of 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.

The following scenarios describe the environments that will be used to implement the capabilities outlined within the project.

Scenario 1: Implementing information-system-integrity capabilities on a discrete manufacturing system

The robotics-based manufacturing workcell 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-based manufacturing workcell includes two small, industrial-grade robots, a supervisory programmable logic controller (PLC), and a safety PLC. Additional information on the robotics-based manufacturing workcell can be found at https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8089.pdf.

Scenario 2: Implementing information-system-integrity capabilities on a process control system

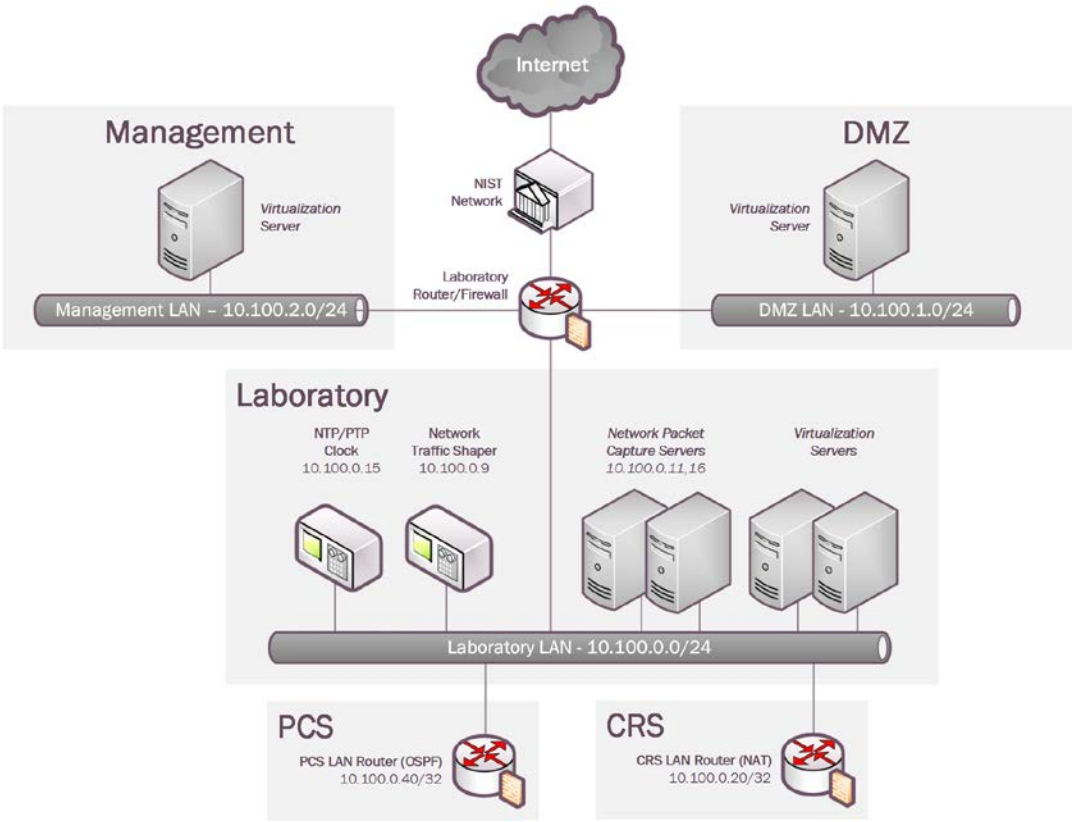
The process control system uses the Tennessee Eastman (TE) control problem as the continuous process model. The TE model is a well-known plant model used in control systems research, and the dynamics of the plant process are well understood. The process must be controlled—perturbations will drive the system into an unstable state. The inherently unstable open-loop operation of the TE process model presents a real-world scenario in which a cyber attack could present a serious risk to human and environmental safety as well as to 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 system can be found at https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8089.pdf.

3 LABORATORY ENVIRONMENT OVERVIEW

The lab contains a shared infrastructure of networked servers, measurement tools, industrial robots, hardware-in-the-loop simulators, and other technologies to support the NIST Cybersecurity Framework Manufacturing Profile implementation on two manufacturing systems: a process control system (PCS) and a collaborative robotics system (CRS). The PCS and CRS employ real-world industrial hardware (e.g., programmable logic controllers, robot arms, sensors), networking devices, and industrial protocols to emulate a process and discrete manufacturing system, respectively. Further details on the two systems are described in Section 4 and Section 5.

The network infrastructure, shown in Figure 3-1, is used for many research functions, including testing, deployment, and hosting of cybersecurity tools; measurement systems for network traffic; creation and manipulation of network traffic for inducing anomalous network activity; and archival storage of experiment data. A virtualization environment was implemented to support the numerous cybersecurity technologies and tools required for the implementation.

Figure 3-1. Lab Network Infrastructure



The lab network infrastructure is separated into three independent network zones: management zone, demilitarized zone (DMZ), and laboratory zone. The management zone contains hosts used to manage the numerous laboratory devices (e.g., network hardware, virtualization servers). The DMZ contains hosts that perform data-sharing functions between the

lab network and the top-level network (in this case, the NIST network). The laboratory zone contains the shared measurement servers and tools and a virtualization infrastructure for hosting cybersecurity tools.

Attached to the laboratory zone are the local PCS and CRS networks, which operate independently of each other. The PCS network accesses the laboratory Local Area Network (LAN) by using the Open Shortest Path First (OSPF) routing protocol, and the CRS accesses the laboratory LAN by using Dynamic network address translation.

A dedicated network packet capture server is provided for both the PCS and CRS. Packets are captured using two methods: packet mirroring and bump-in-the-wire network probes. Packet mirroring involves configuring network devices (e.g., routers, switches) to duplicate and forward the packet to another port. Network probes perform a similar function, but they must be physically connected to the network cable. In the lab, mirrored packets are aggregated into two streams (one containing PCS traffic and the other containing CRS traffic) by using a packet broker. Network traffic from the aggregator and network probes terminate at the network packet capture servers where they are buffered, stored, and later processed to calculate the metrics and key performance indicators required for experimental analysis.

4 Collaborative Robotics System

The CRS workcell, shown in Figure 4-1, contains two robotic arms that perform a material handling process called machine tending. Robotic machine tending utilizes robots to interact with machinery, performing physical operations that a human operator would normally perform (e.g., loading and unloading parts in a machine, opening and closing machine doors, and activating operator control panel buttons).

Figure 4-1. The CRS workcell in standby, waiting for the operator to initiate the manufacturing process, with the operator control panel visible at the top of the figure

A human operator interfaces with the workcell through a human-machine interface (HMI) and a control panel external to the work area.

The workcell was designed and constructed to be reconfigurable, allowing numerous types of operational methodologies, network topologies, and industrial networking protocols to be investigated. The two robots collaborate to transport parts through the manufacturing process, as a single robot cannot physically reach all four stations. Having two robots also increases workcell efficiency.

Control System Operation

Parts are transported by the robot arms through four simulated machining operations, known as *stations*. Each station is composed of a fixture for holding the part, an infrared proximity sensor for detecting the part, a single-board computer simulating the actions and communications of a typical machining center, and a liquid crystal display for displaying the operational status of the station. The stations communicate with the supervisory PLC over the workcell LAN. The supervisory PLC monitors and controls all aspects of the manufacturing process.

Manufacturing data from the four machining stations are used by the PLC to determine what operations, known as *jobs*, the robots must perform to keep the parts moving through the sequential manufacturing process. The PLC also communicates with the HMI for operator visibility and control.

The workcell is supported by a shared infrastructure of networked servers, measurement tools, and other technologies. The infrastructure is used for many research functions, including testing, deployment, and hosting of cybersecurity tools; measurement and packet capture systems for network traffic; creation and manipulation of network traffic for inducing anomalous network activity; and archival storage of experiment data. A virtualized server

infrastructure was installed to support the numerous cybersecurity technologies and tools required for the implementation.

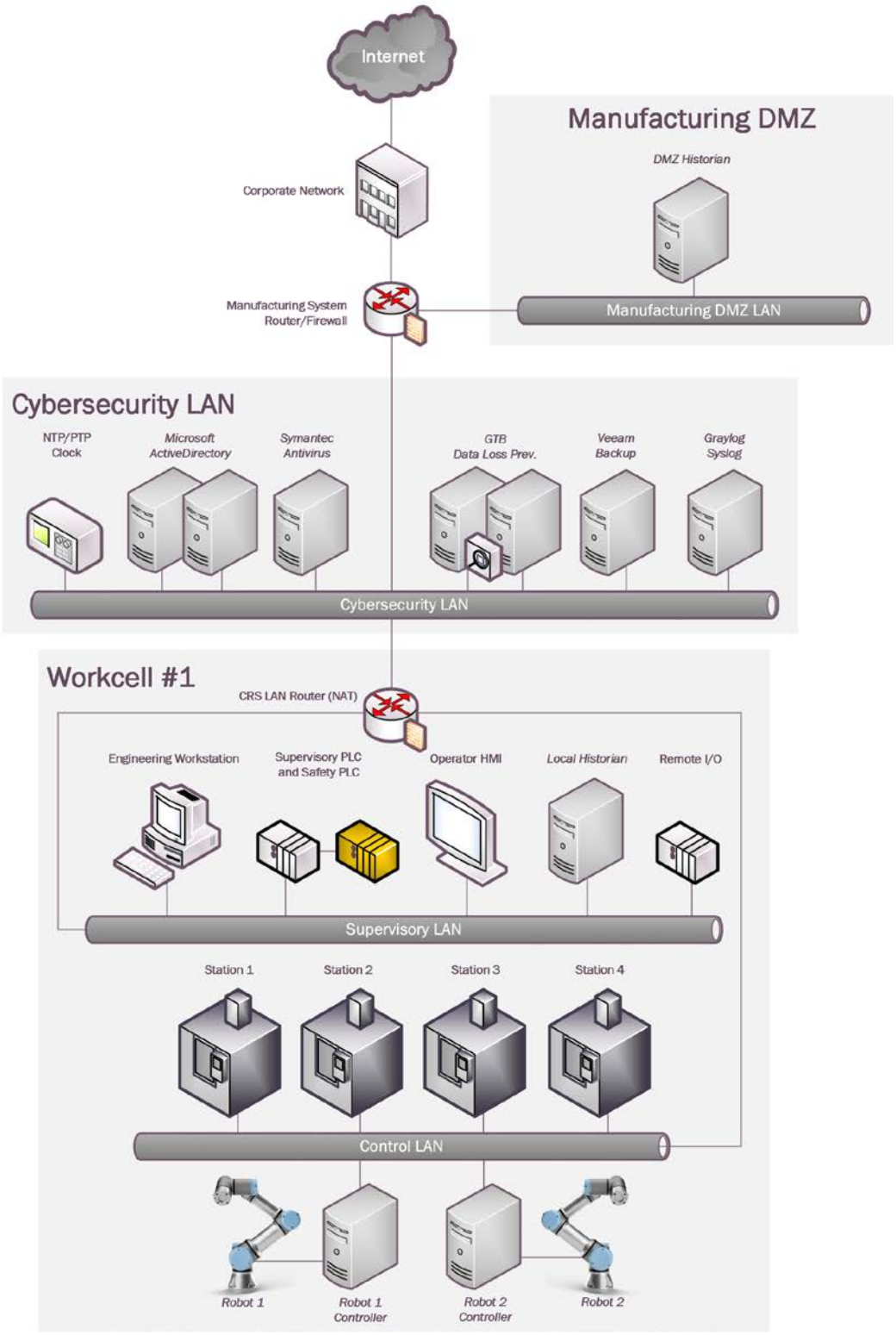
Network Architecture

The CRS network, shown in Figure 4-2, is hierarchically architected, separating the devices performing supervisory functions from the devices controlling the manufacturing process. The workcell top-level router is a Siemens RUGGEDCOM RX1510 and provides firewall capabilities for rule-based allowance and restriction of network traffic. The router is connected to the laboratory LAN by using NAT. Layer 2 network traffic for the supervisory LAN is handled by a Netgear GS724T managed Ethernet switch, and network traffic for the control LAN is handled by a Siemens i800 managed Ethernet switch.

The router and network switches are configured to mirror all incoming network traffic to a packet capture server located in the measurement rack. In-line (i.e., bump-in-the-wire) network probes are located at the PLC, HMI, and Station 1 to provide dedicated forwarding of all incoming and outgoing network traffic to the packet capture server.

The primary industrial network protocol utilized by the manufacturing process components is Modbus TCP.

Figure 4-2. CRS Network Architecture



Additional information on the robotics-based manufacturing workcell can be found at https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8089.pdf.

5 PROCESS CONTROL SYSTEM

The PCS emulates an industrial continuous manufacturing system, a manufacturing process to produce or process materials continuously where the materials are constantly moving, chemically reacting, or undergoing mechanical or thermal treatment. Continuous manufacturing usually implies a 24/7 operation with infrequent maintenance shutdowns, contrasted with batch manufacturing. Examples of continuous manufacturing systems are chemical production, oil refining, natural gas processing, and wastewater treatment.

The PCS uses the TE challenge problem, a real-world industrial chemical manufacturing process, as the simulation model for the chemical reaction. The system integrates the control algorithm developed by Ricker to control the simulated chemical reaction. With the use of widely deployed industrial hardware like PLCs and industrial network switches as part of the control loop, this system emulates a complete setup of a continuous chemical manufacturing system. This hardware-in-the-loop configuration allows the test bed to measure performance of the manufacturing system by using real-world industrial hardware, while the chemical manufacturing process is simulated in software.

Control System Operation

The PCS includes a software simulator to emulate the TE chemical-reaction process. The simulator is written in C code and is executed on a Windows 7-based computer. In addition, the system includes a PLC, a software controller implemented in MATLAB, an HMI, an Object Linking and Embedding for process control (OPC) Data Access (DA) server, a data historian, an engineering workstation, and several virtual local area network (VLAN) switches and network routers.

The TE plant simulator requires a controller to provide the control loops to operate continuously. A decentralized controller implemented in Simulink, developed by Ricker, is used as the process controller. The Ricker implementation matches the plant simulator accurately, and the controller is a separate software process that runs on a computer separate from the plant simulator.

To provide communication between the plant simulator and the controller, a hardware PLC with industrial network protocol capability is used. The industrial protocol is used to communicate between the plant simulator and the PLC. The plant simulator sends its sensor information to the controller, and the controller algorithm uses the sensor inputs to compute the desired values of the actuators and sends them back to the plant simulator.

In the plant simulator computer, a multinode DeviceNet card was installed. DeviceNet is a common industrial protocol used in the automation industry to exchange data between control devices. The multinode card allows a single hardware device to emulate multiple virtual DeviceNet nodes. In our case, each sensor and actuator point is a dedicated node. Therefore, 53 virtual nodes (41 for sensors and 12 for actuators) were configured in the system. A software interface was developed to send and receive sensor and actuator values between the plant simulator and the PLC through DeviceNet.

An OPC DA server runs on a Windows 7 computer, acting as the main data gateway for the PLC. The PLC communicates to the OPC DA server to update and retrieve all the sensor and actuator information, respectively. This sensor and actuator information is also known in PLC terminology as a "tag." The controller has a MATLAB Simulink interface that communicates with the OPC DA server directly.

An HMI and a data historian are implemented in the system. The HMI provides a graphical user interface to present information to an operator or user about the state of the process. The data historian serves as the main database to record all the process sensor and actuator information. Both HMI and data historian have built-in interfaces to establish connections to the OPC DA to access all the process information.

An engineering workstation is used in the system for engineering support, such as PLC development and control, HMI development and deployment, and data-historian data retrieval.

Network Architecture

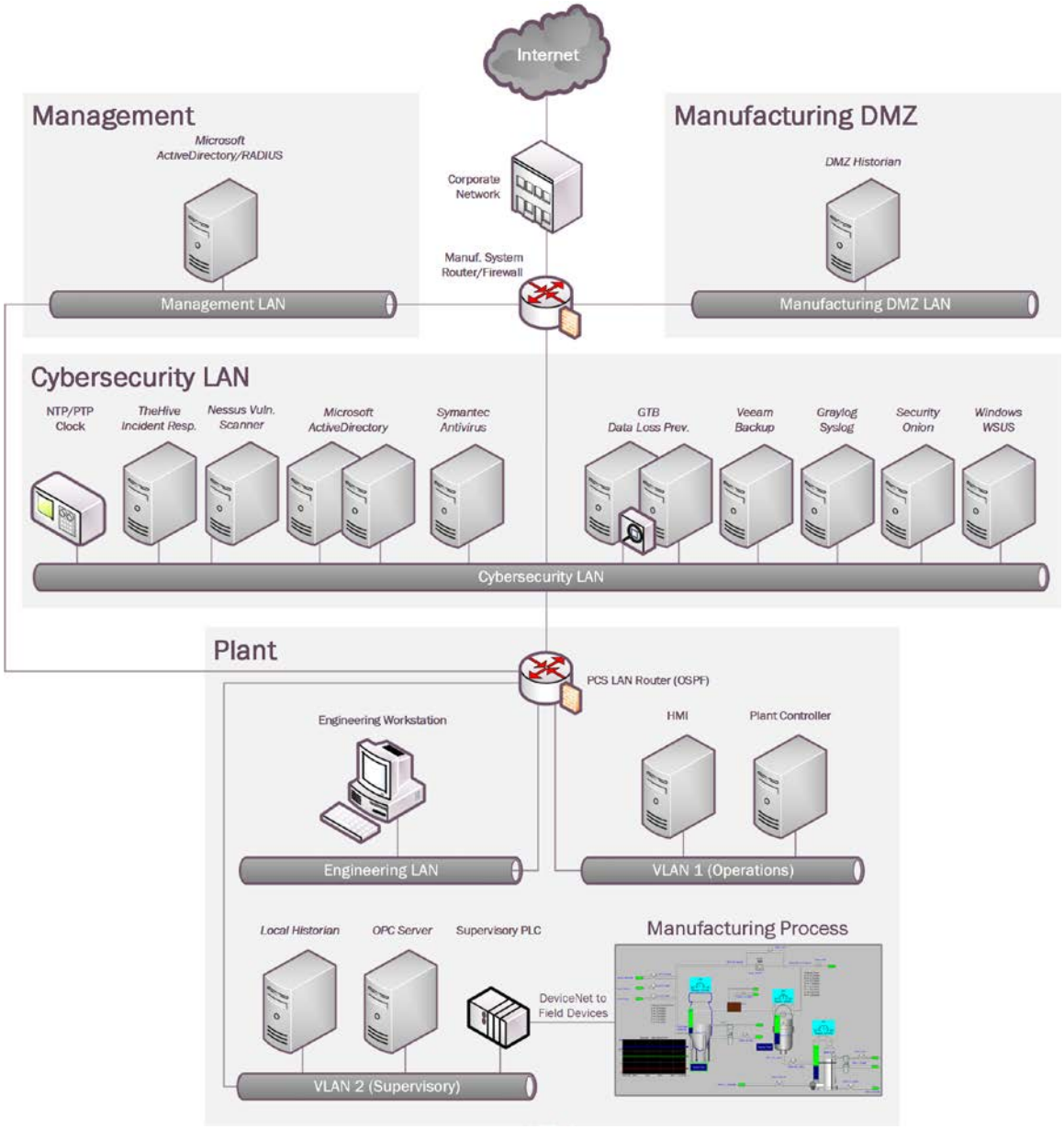
The PCS network is segmented from the main laboratory LAN by a boundary router. The router uses a dynamic routing protocol, OSPF, to communicate with the main top-level router. The network architecture is shown in Figure 5-1.

All network traffic needs to go through the boundary router to access the main laboratory LAN.

There are two virtual network segments in the system. Each network is managed by an Ethernet switch. The HMI and the controller are in VLAN-1, while the plant simulator, data historian, OPC DA server, and PLC are in VLAN-2.

VLAN-1 simulates a central control-room environment where the HMI and the controllers are virtually located in the same network segment. VLAN-2 simulates the process operation environment, which typically consists of the operating plant, PLCs, OPC server, and data historian.

Figure 5-1. PCS Network Architecture



Additional information on the process control system and the TE process can be found at https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8089.pdf.

6 Desired Capabilities and Component List

The following system capabilities are desired:

- tracking approved software applications that are permitted to be present and active on the network
- continuously monitoring a network for unusual events or data packet trends process of identifying, monitoring, recording, and analyzing security events or incidents within a real-time OT environment
- detecting malicious software designed to damage a computer, server, computer network, or industrial controller
- monitoring for unapproved changes, that all changes are documented, and that services are not unnecessarily disrupted
- validating access to the ICS network by authenticated users
- validating operating system and application software file integrity

The system is composed of the following components:

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

7 Relevant Standards and Guidance

- A. Sedgewick et al., *Guide to Application Whitelisting,* NIST SP 800-167, NIST, Oct. 2015. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-167.pdf.
- Department of Homeland Security, *Critical Manufacturing Sector Cybersecurity Framework Implementation Guidance,* 2015. Available: https://www.cisa.gov/sites/default/files/publications/critical-manufacturing-cybersecurity-framework-implementation-guide-2015-508.pdf.
- Executive Order no. 13636, *Improving Critical Infrastructure Cybersecurity,* DCPD-201300091, Feb. 12, 2013. Available: http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.
- NIST, *Framework for Improving Critical Infrastructure Cybersecurity,* Feb. 12, 2014. Available: https://doi.org/10.6028/NIST.CSWP.02122014
- J. J. Downs and E. F. Vogel, "A Plant-wide Industrial Problem Process," Comput. Chem. Eng., vol. 17, no. 3, 1993, pp. 245–255.
- J. McCarthy et al., *Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection,* NIST Interagency Report (NISTIR) 8219, NIST, Nov. 2018. Available: https://www.nccoe.nist.gov/sites/default/files/library/mf-ics-nistir-8219.pdf.
- K. Stouffer et al., *Cybersecurity Framework Manufacturing Profile,* NIST Internal Report 8183, NIST, May 2017. Available: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf.

- M. J. Stone et al., "Data Integrity: Reducing the impact of an attack," white paper, NIST, Nov. 23, 2015. Available: https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/data-integrity-project-description-draft.pdf.
- NIST, *Cybersecurity Framework*. Available: http://www.nist.gov/cyberframework/.
- R. Candell et al., *An Industrial Control System Cybersecurity Performance Testbed,* NISTIR 8089, NIST, Nov. 2015. Available: http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8089.pdf.
- *Security and Privacy Controls for Federal Information Systems and Organizations,* NIST SP 800-53 Revision 4, NIST, Apr. 2013. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.
- W. Newhouse et al., *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework,* NIST SP 800-181, Aug. 2017. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

8 Security Control Map

Table 8-1 maps the characteristics of the commercial products that the NCCoE will apply to this cybersecurity challenge to the applicable standards and best practices described in the Framework for Improving Critical Infrastructure Cybersecurity and to other NIST activities. This exercise is meant to demonstrate the real-world applicability of standards and best practices but does not imply that products with these characteristics will meet an industry's requirements for regulatory approval or accreditation.

Table 8-1. Security Control Map

NIST Cybersecurity Framework Version 1.1				Sector-Specific Standards and Best Practices				
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 4**	**CCS CSC**	**COBIT 5**	**ISA 62443-2-1:2009**	**ISA 62443-3-3:2013**	**ISO/IEC 27001:2013**
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users.	AC-2, IA Family	16	DSS05.04, DSS06.03	4.3.3.5.1	SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3
		PR.AC-2: Physical access to assets is managed and protected.	PE-3, PE-8, PE-9	n/a	DSS01.04, DSS05.05	4.3.3.3.2	n/a	A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3

NIST Cybersecurity Framework Version 1.1				Sector-Specific Standards and Best Practices				
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 4**	**CCS CSC**	**COBIT 5**	**ISA 62443-2-1:2009**	**ISA 62443-3-3:2013**	**ISO/IEC 27001:2013**
		PR.AC-3: Remote access is managed.	AC-17, AC-19, AC-20, SC-15	n/a	APO13.01, DSS01.04, DSS05.03	4.3.3.6.6	SR 1.13, SR 2.6	A.6.2.2, A.13.1.1, A.13.2.1
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties.	AC-14, AC-2, AC-5, AC-6	12, 15	n/a	4.3.3.7.3	SR 2.1	A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate.	AC-4, SC-7	n/a	n/a	4.3.3.4	SR 3.1, SR 3.8	A.13.1.1, A.13.1.3, A.13.2.1
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect	**PR.DS-1:** Data at rest is protected.	SC-28	17	APO01.06, BAI02.01, BAI06.01, DSS06.06	n/a	SR 3.4, SR 4.1	A.8.2.3
		PR.DS-2: Data in transit is protected.	SC-8	17	APO01.06, DSS06.06	n/a	SR 3.1, SR 3.8, SR 4.1	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3

NIST Cybersecurity Framework Version 1.1				Sector-Specific Standards and Best Practices				
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 4**	**CCS CSC**	**COBIT 5**	**ISA 62443-2-1:2009**	**ISA 62443-3-3:2013**	**ISO/IEC 27001:2013**
	the confidentiality, integrity, and availability of information.	**PR.DS-3:** Assets are formally managed throughout removal, transfers, and disposition.	CM-8, MP-6, PE-16	n/a	BAI09.03	4.4.3.3.3.9	SR 4.2	A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7
		PR.DS-4: Adequate capacity to ensure availability is maintained.	AU-4, CP-2, SC-5	n/a	APO13.01	n/a	SR 7.1, SR 7.2	A.12.3.1
		PR.DS-5: Protections against data leaks are implemented.	AC-4, PE-19, PS-6, SC-7, SI-4	17	APO01.06	n/a	SR 5.2	A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3

NIST Cybersecurity Framework Version 1.1				Sector-Specific Standards and Best Practices				
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 4**	**CCS CSC**	**COBIT 5**	**ISA 62443-2-1:2009**	**ISA 62443-3-3:2013**	**ISO/IEC 27001:2013**
		PR.DS-6: Integrity-checking mechanisms are used to verify software, firmware, and information integrity.	SI-7	n/a	n/a	n/a	SR 3.1, SR 3.3, SR 3.4	A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3
		PR.DS-7: The development and testing environment(s) are separate from the production environment.	CM-2	n/a	BAI07.04	n/a	n/a	A.12.1.4
DETECT (D)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner, and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed.	CM-2	n/a	DSS03.01	4.4.3.3	n/a	n/a
		DE.AE-2: Detected events are analyzed to understand attack targets and methods.	AU-6, IR-4	n/a	n/a	4.3.4.5.6	SR 2.8, SR 2.9	A.16.1.1, A.16.1.4

NIST Cybersecurity Framework Version 1.1				Sector-Specific Standards and Best Practices				
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 4**	**CCS CSC**	**COBIT 5**	**ISA 62443-2-1:2009**	**ISA 62443-3-3:2013**	**ISO/IEC 27001:2013**
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors.	AU-6, AU-12, IR-5	n/a	n/a	n/a	SR 6.1	n/a
		DE.AE-4: Impact of events is determined.	IR-4, RA-3, SI-4	n/a	APO12.06	n/a	n/a	n/a
		DE.AE-5: Incident alert thresholds are established.	IR-4, IR-5, IR-8, AU-3	n/a	APO12.06	4.2.3.10	n/a	n/a
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events.	AC-2, AU-12, CA-7, SC-7, SI-4	14, 16	DSS05.07	n/a	SR 6.2	n/a
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events.	CA-7, PE-3, PE-6	n/a	n/a	4.3.3.3.8	n/a	n/a
		DE.CM-3: Personnel activity is monitored to detect cybersecurity events.	AC-2, AU-12, AU-13, CA-7, CM-10, CM-11	n/a	n/a	n/a	SR 6.2	A.12.4.1

NIST Cybersecurity Framework Version 1.1				Sector-Specific Standards and Best Practices				
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 4**	**CCS CSC**	**COBIT 5**	**ISA 62443-2-1:2009**	**ISA 62443-3-3:2013**	**ISO/IEC 27001:2013**
		DE.CM-4: Malicious code is detected.	SI-3	5	DSS05.01	4.3.4.3.8	SR 3.2	A.12.2.1
		DE.CM-5: Unauthorized mobile code is detected.	SC-18	n/a	n/a	n/a	SR 2.4	A.12.5.1
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.	CA-7, PS-7, SA-4, SA-9, SI-4, MA-5	n/a	APO07.06	n/a	n/a	A.14.2.7, A.15.2.1
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	CA-7, CM-3, CM-8, SI-4	n/a	n/a	n/a	n/a	n/a
		DE.CM-8: Vulnerability scans are performed.	RA-5	n/a	BAI03.10	4.2.3.1	n/a	A.12.6.1
	Detection Processes (DE.DP): Detection processes and procedures are maintained and	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability.	CA-2, CA-7, PM-14	5	DSS05.01	4.4.3.1	n/a	A.6.1.1

NIST Cybersecurity Framework Version 1.1				Sector-Specific Standards and Best Practices				
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 4**	**CCS CSC**	**COBIT 5**	**ISA 62443-2-1:2009**	**ISA 62443-3-3:2013**	**ISO/IEC 27001:2013**
	tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-2:** Detection activities comply with all applicable requirements.	CA-2	n/a	n/a	4.4.3.2	n/a	A.18.1.4
		DE.DP-3: Detection processes are tested.	PM-14	n/a	APO13.02	4.4.3.2	SR 3.3	A.14.2.8
		DE.DP-4: Event detection information is communicated to appropriate parties.	AU-6, SI-4	n/a	APO12.06	4.3.4.5.9	SR 6.1	A.16.1.2
		DE.DP-5: Detection processes are continuously improved.	CA-2, CA-7, PL-2, RA-5, SI-4, PM-14	n/a	APO11.06, DSS04.05	4.4.3.4	n/a	A.16.1.6

APPENDIX A REFERENCES

[1] K. Stouffer et al., *Guide to Industrial Control Systems (ICS) Security,* National Institute of Standards and Technology Special Publication 800-82 Revision 2, Gaithersburg, Md., May 2015. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

APPENDIX B ACRONYMS AND ABBREVIATIONS

AC	Access Control
AE	Anomalies and Events
CM	Continuous Monitoring
CRS	Collaborative robotics system
DE	Detect
DMZ	Demilitarized Zone
DP	Detection Processes
DS	Data Security
EL	Engineering Laboratory
HMI	Human-Machine Interface
ICS	Industrial Control System(s)
IT	Information Technology
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
OPC	Object Linking and Embedding for Process Control
OSPF	Open Shortest Path First
OT	Operational Technology
PCS	Process Control System
PLC	Programmable Logic Controller
PR	Protect
SP	Special Publication
TE	Tennessee Eastman