PROJECT DESCRIPTION

DETECTING AND PROTECTING AGAINST DATA INTEGRITY ATTACKS 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

DRAFT

June 2019

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.

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 in the 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 white-listing, 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 unlicensed 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 robotics-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, Cybersecurity Framework, file integrity checking mechanisms, industrial control systems, malware detection and mitigation, manufacturing, security incident and event monitoring, unauthorized software

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 NIST or NCCoE, 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://www.nccoe.nist.gov.

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

Public comment period: June 12, 2019 to July 25, 2019

TABLE OF CONTENTS

1 Executive Summary

Purpose

Industrial control systems in manufacturing environments are increasingly subject to cyber attacks and insider threats. To enhance system security, manufacturing organizations must be able to protect and detect against data integrity attacks. Such threats to data integrity could compromise critical manufacturing programs, decrease productivity, and negatively impact safety and business operations should a cyber incident occur. This project will provide a comprehensive approach that manufacturing organizations can use to address the challenge of protecting and detecting against data integrity attacks by leveraging the following cybersecurity capabilities: behavioral anomaly detection, security incident and event monitoring, industrial control system (ICS) application white listing, 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 data 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

The objectives of this project are to:

- provide a proposed approach to prevent, mitigate, and detect threats from cyber attacks 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

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

- What capabilities are needed to prevent unwanted data modifications within ICS that use functionality verification, data integrity checking, intrusion detection, malicious code detection, and security alert and advisory controls requirements?
- What protections are needed for controlling modifications to hardware, firmware, and software, and what documentation is needed to ensure that 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?

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
- the use of white listing 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 not authorized use of the system
- file integrity monitoring to validate the integrity of operating systems and application software files
- behavioral anomaly detection tools to continuously monitor the network for unusual events or trends
- malware detection and mitigation of any software intentionally designed to damage a computer, server, or computer network

Assumptions

A manufacturing lab infrastructure is in place at NIST that represents a typical manufacturing environment as demonstrated in the Robotic Assembly Enclave Network and Process Control System Architectures below (Figure 1 and Figure 2). Numerous commercially available off-the-shelf technologies exist in the market to demonstrate the example solutions.

Challenges

Although the lab for this build represents a typical manufacturing environment, the lab is on a smaller scale than many commercial manufacturing environments and does not contain the number of devices that would typically be found in a real-world setting (see Robotics and Process Control System diagrams in Section 3).

While the lab environment simulates a real-world setting, it is important to note that the lab environment likely provides a limited representation of real-world manufacturing environments, especially regarding the number of devices being used (see Robotics and Process Control System diagrams in Section 3).

Background

As stated in NIST Special Publication (SP) 800-82*, Guide to Industrial Control Systems 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 to solve these challenges by developing reference designs and the practical application of cybersecurity technologies. This project will build upon NIST Interagency 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 ICS workshop, held at NIST 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 robotics-based manufacturing process

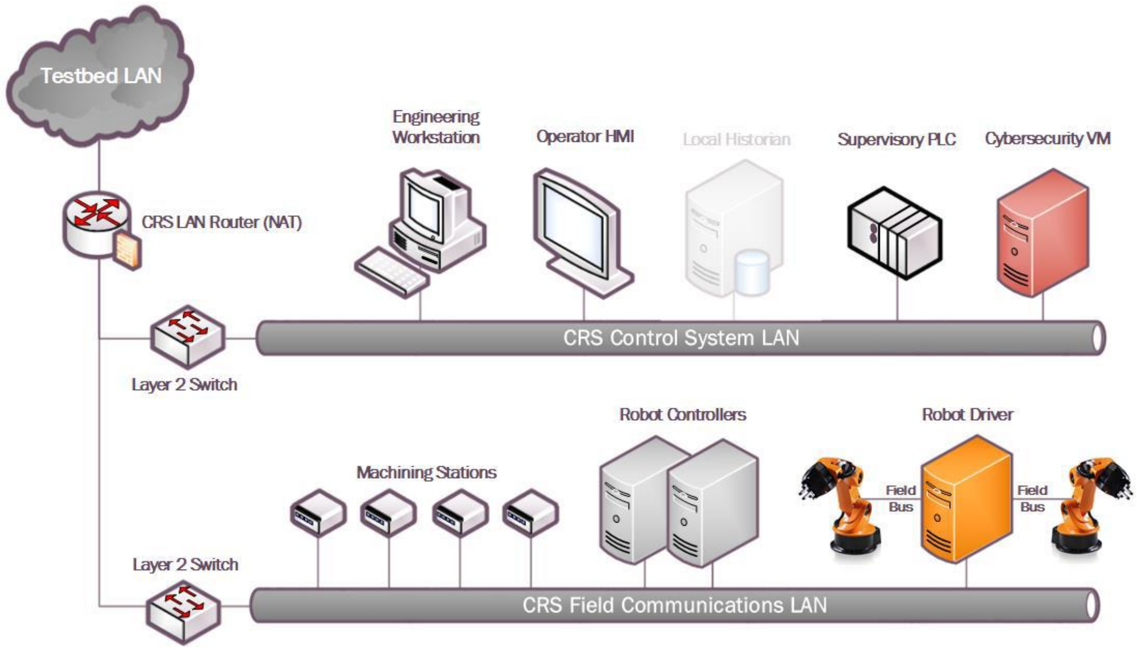
The robotics-based manufacturing workcell contains a robotic assembly system in which industrial robots work cooperatively to move parts through a simulated manufacturing operation. The robots work according to a plan that changes dynamically based on process feedback. The robotics-based manufacturing 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 continuous 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 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 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 Robotic Assembly Enclave Network Architectures

Figure 1. Robotics-Based Manufacturing Workcell Architecture



The network design of the robotics enclave is shown in Figure 1. The robotics enclave is designed as a local area network, using the EtherCAT real-time industrial protocol for communication between the controller and the robots.

The robotics enclave is designed similar to the TE model in that different functions of the robotics system are encapsulated in more than one subnet. As with the TE model, the robotics enclave serves to validate the requirements specified in the prevalent security standards.

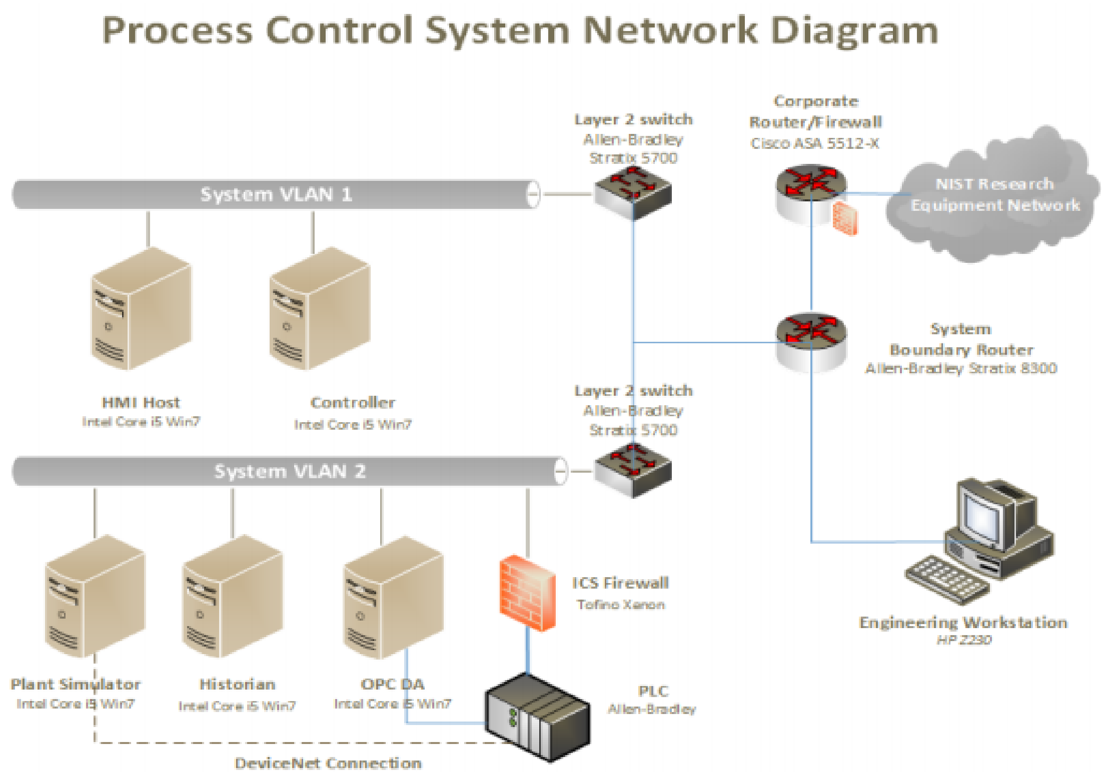
Additional information on the robotics-based manufacturing workcell can be found at https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8089.pdf.

Process Control System

The process control system (PCS) enclave emulates an industrial continuous manufacturing system, a manufacturing process to produce or process materials continuously, where the materials are continuously moving, going through chemical reactions, or undergoing mechanical or thermal treatment.

Continuous manufacturing usually implies a 24/7 operation with infrequent maintenance shutdowns and is contrasted with batch manufacturing. Examples of continuous manufacturing systems are chemical production, oil refining, natural-gas processing, and wastewater treatment. An architecture of the PCS network is depicted in the above Figure 2.

Figure 2. Process Control System Architecture



The TE control problem was chosen as the continuous process model for a number of reasons. First, the TE model is a well-known plant model used in control systems research, and the dynamics of the plant process are well understood. Second, the process must be controlled; otherwise, 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 represent a real risk to human safety, environmental safety, and economic viability. Third, the process is complex and nonlinear and has many degrees of freedom by which to control and perturb the dynamics of the process.

And finally, numerous simulations of the TE process have been developed with readily available reusable code. We chose the University of Washington Simulink controller design by Ricker for its multiloop control architecture, making distributed control architectures viable. It accurately matches the Downs and Vogel model, and the control code is easily separable from the plant code.

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

Component List

The PCS is comprised of the following components:

- ICS application white-listing tools
- ICS behavioral anomaly detection tools
- security incident and event monitoring

- malware detection and mitigation
- change control management
- access control
- file-integrity-checking mechanisms
- user authentication and authorization

Desired Capabilities

The following system capabilities are desired:

- tracking of approved software applications that are permitted to be present and active on the network
- continuous monitoring of 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
- detection of malicious software designed to cause damage to a computer, server, or computer network
- monitoring for unapproved changes, that all changes are documented, and that services are not unnecessarily disrupted
- validation of access to the ICS network by authenticated users
- validation of operating system and application software file integrity

4 Relevant Standards and Guidance

- A. Sedgewick et al., Guide to Application Whitelisting, NIST SP 800-167, Gaithersburg, Md., Oct. 2015. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-167.pdf
- Critical Manufacturing Sector Cybersecurity Framework Implementation Guidance, Department of Homeland Security, 2015. Available: https://www.dhs.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
- Framework for Improving Critical Infrastructure Cybersecurity, NIST, Gaithersburg, Md., Feb. 12, 2014. Available: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf
- 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, NISTIR 8219, NIST, Gaithersburg, Md., 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, NISTIR 8183, Gaithersburg, Md., Sep.. 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, Gaithersburg, Md., 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, NIST Interagency/Internal (IR) 8089, Gaithersburg, Md., 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, 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, Gaithersburg, Md., Aug. 2017. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

5 Security Control Map

This table 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.

296 **Table 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
		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

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-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 the confidentiality, integrity, and availability of information.	**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
		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

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-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
		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

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**
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
		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	**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

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**
	and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**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
		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

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-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 tested to ensure timely and adequate awareness of anomalous events.	**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
		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

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.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 (NIST) Special Publication (SP) 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

AE	Anomalies and Events
CM	Continuous Monitoring
D	Detect
DP	Detection Processes
EL	Engineering Laboratory
ICS	industrial control systems
IR	Interagency/Internal
IT	information technology
NCCoE	National Cybersecurity Center of Excellence
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
OT	operational technology
PCS	process control system
PLC	programmable logic controller
PR	Protect
TE	Tennessee Eastman