PROJECT DESCRIPTION

RESPONDING TO AND RECOVERING FROM A CYBER ATTACK

Cybersecurity for the Manufacturing Sector

Michael Powell

National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Michael Pease
Keith Stouffer
CheeYee Tang
Timothy Zimmerman

Communications Technology Laboratory
National Institute of Standards and Technology

John Hoyt
Stephanie Saravia
Aslam Sherule
Barbara Ware
Lynette Wilcox
Kangmin Zheng

The MITRE Corporation
McLean, Virginia

DRAFT

February 2022

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 https://www.nccoe.nist.gov/. To learn more about NIST, visit https://www.nist.gov/.

This document focuses on a manufacturing sector problem, responding and recovering from data integrity attack which is also relevant to many industry sectors. 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 incorporated by manufacturing sector organizations.

Abstract

Industrial control systems (ICS) and devices that run manufacturing environments play a critical role in the supply chain. Manufacturing organizations rely on ICS to monitor and control physical processes that produce goods for public consumption. These same systems are facing an increasing number of cyber attacks, presenting a real threat to safety and production, and economic impact to a manufacturing organization. Though defense-in-depth security architecture helps to mitigate cyber risks to some extent, it cannot guarantee elimination of all cyber risks; therefore, manufacturing organizations should also have a plan to recover and restore manufacturing operations should a cyber attack impact the plant operation. The goal of this project is to demonstrate a means to recover equipment from cyber attacks and restore operations. The NCCoE, part of NIST's Information Technology Laboratory, in conjunction with the NIST Communications Technology Laboratory (CTL) and industry collaborators, will demonstrate an approach for responding to and recovering from an ICS attack within the manufacturing sector by leveraging the following cybersecurity capabilities: event reporting, log review, event analysis, and incident handling and response. The NCCoE and the CTL 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 commercial off the shelf (COTS) based modular security controls for manufacturers. NCCoE will implement each of the listed capabilities in a discrete-based manufacturing work-cell that emulates a typical manufacturing process. This project will result in a freely available NIST Cybersecurity Practice Guide.

Keywords

response; recovery; restoration; industrial control systems; operational technology

Acknowledgements

The NCCoE would like to thank Dragos for their discussion of response and recovery during the development of this project description.

Disclaimer

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 https://www.nccoe.nist.gov/.

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

Public comment period: February 28, 2022 to April 14, 2022

Table of Contents

1 EXECUTIVE SUMMARY

Purpose

This document defines an NCCoE project focused on responding to and recovering from a cyber attack within an Industrial Control System (ICS) environment. Manufacturing organizations rely on ICS to monitor and control physical processes that produce goods for public consumption. These same systems are facing an increasing number of cyber attacks resulting in a loss of production from destructive malware, malicious insider activity, or honest mistakes. This creates the imperative for organizations to be able to quickly, safely, and accurately recover from an event that corrupts or destroys data (such as database records, system files, configurations, user files, application code).

The purpose of this NCCoE Project is to demonstrate how to operationalize the NIST Framework for Improving Critical Infrastructure Cybersecurity (CSF) Functions and Categories in a scaled-down version of targeted manufacturing industrial environments. Multiple systems need to work together to recover when data integrity is compromised. This project explores methods to effectively restore data corruption in commodity components (applications and software configurations) as well as custom applications and data. The NCCoE—in collaboration with members of the business community and vendors of cybersecurity solutions—will identify standards-based, commercially available and open-source hardware and software components to design a manufacturing lab environment to address the challenge of responding to and recovering from a cyber attack of an ICS environment.

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

This project will demonstrate how to respond to and recover from a cyber attack within an ICS environment. Once a cybersecurity event is detected, typically the following tasks take place before the event is satisfactorily resolved.

1. Event reporting
2. Log review
3. Event analysis
4. Incident handling and response
5. Eradication and Recovery

NIST *Cybersecurity Framework* Respond and Recover functions and categories are used to guide this project. The objective of NIST *Cybersecurity Framework* Respond function is to develop and implement the appropriate activities to take action regarding a detected cybersecurity event. The objective of Recover function is to develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Out of scope for this project is systems such as enterprise resource planning (ERP), manufacturing resource planning (MRP), manufacturing execution systems (MES) that operate on traditional IT infrastructures that runs on Windows or Linux OS. These IT systems have well documented recovery tools available including those documented in NIST Cybersecurity Practice Guide SP 1800-11, *Data Integrity: Recovering from Ransomware and Other Destructive Events.*

Assumptions

This project assumes that the attack is discovered after impact has occurred or immediately prior to impact occurring. It is assumed that the adversary has done preliminary work to gain access, perform discovery, and lateral movement as needed to setup for each scenario. A comprehensive security architecture should be designed to catch an adversary during all steps of the kill chain including initial access, discovery, and lateral movement. However, a comprehensive defense should also be prepared to restore and recover in the event that an adversary is not detected until it is too late. This guide focuses on the, hopefully rare, event of an adversary causing an impact.

This project assumes:

- The effectiveness of the example solutions are independent of the scale of the manufacturing environment.
- The lab infrastructure this project will be executed in has a relatively small number of robotic and manufacturing process nodes, but it is assumed that the example solutions will be effective if the number of ICS components increases to levels that are realistic for actual production environments.
- This project focuses on the Respond and Recover portions of the NIST *Cybersecurity Framework*. It is assumed that the Identify, Detect, and Protect functions have been implemented to some maturity level, and the following capabilities are operationalized including the necessary technologies:
    - Physical access to the site is managed and protected.
    - ICS assets are segmented from IT assets via an industrial DMZ.
    - Authentication and Authorization mechanisms for accessing ICS assets are in place.
    - Remote access to the ICS environment and ICS assets is fully managed.
    - Asset and vulnerability management tool is operationalized.
    - Behavior analysis detection tool is operationalized.
    - IT Network protection measures (such as firewalls, segmentation, intrusion detection, etc.) are in place.
    - Vulnerabilities associates with the supply chain and vendor access have been addressed.
    - People and processes that support back up and overall enterprise incident response plans are in place.

Challenges

Implementations that provide recovery solutions and procedures need to acknowledge that restoration procedures that involve the use of backups are designed to restore the system to some previous state, but the 'last known good state' may not necessarily be free of vulnerabilities.

- Vulnerabilities may exist in backup data.
- Backup data may be compromised while in storage.
- Dormant or inactive malware may exist in backup data.

Background

Manufacturing systems are often interconnected and mutually dependent systems and are essential to the nation's economic security. ICS that run in manufacturing environments are vital to the operation of the nation's critical infrastructures and essential to the nation's economic security. It is critical for the stakeholders of the enterprises in the manufacturing sector to consider how adversaries could affect the operations of their plant and safety of the people and property. 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 500 market leaders to smaller companies specializing in ICS security. The aim is to solve these challenges by demonstrating practical applications of cybersecurity technologies in a scaled-down version of a manufacturing environment.

Considering the current era of Industry 4.0, enterprises are connecting business systems and IT networks to ICS networks to improve business agility and operational efficiency. However, recent attacks on ICS have shown that the cyber criminals are pivoting into the ICS environment from the business systems and IT networks. Most ICS systems have been historically isolated from the business systems and IT networks, and therefore, were not designed to withstand cyber attacks. The cyber risk mitigation technologies used in the IT networks are often not suitable for ICS networks because of the real-time and deterministic nature of the ICS. This project will provide guidance for manufacturing organizations to design environments incorporating cyber attack risk mitigation appropriate for ICS cybersecurity concerns.

This project will build upon NIST Special Publication 1800-10: *Protecting Information and System Integrity in Industrial Control System Environments* by identifying and demonstrating capabilities to improve Response to and Recovery from cyber attacks in the ICS environment.

2 Cybersecurity Capabilities to be Demonstrated

This project will demonstrate an approach for responding to and recovering from an ICS attack within the manufacturing sector. The cybersecurity capabilities listed below are the typical sequential tasks that takes place as part of an Incident Response and Recovery process once a cybersecurity event is detected.

1. Event reporting
2. Log review
3. Event analysis
4. Incident handling and response
5. Eradication and Recovery

Leveraging these cybersecurity capabilities facilitates a satisfactory resolution of a cyber attack event. A brief summary of these capabilities and the NIST *Cybersecurity Framework* subcategory that maps to these capabilities are summarized below. These capabilities are described in detail in ISA/IEC 62443-2-1, *Security Program Requirements for IACS Asset Owners*. ISA/IEC 62443 is a collection of international standards for ICS cybersecurity published by International Society of Automation (http://www.isa.org).

Event Reporting

Once an event is detected, it should be reported to the appropriate personnel and assigned appropriate priority for handling to ensure that awareness of security risks are generated so that necessary action can be taken in a timely manner. Events should be evaluated to determine who should receive them and their priority. Once the determination is made, the system should be configured to have the events reported appropriately.

CSF Category	CSF Subcategory ID	CSF Subcategory Requirements
Detection Processes	DE.DP-4	Event detection information is communicated
Communications	RS.CO-2	Incidents are reported consistent with established criteria
	RS.CO-3	Information is shared consistent with response plans
	RS.CO-4	Coordination with stakeholders occurs consistent with response plans

Log Review

Events should be written to one or more protected event/audit logs and retained for an adequate time period. Logging events is a primary means for reviewing and analyzing events. Retaining event/audit logs provides support for forensics, which allows identification of root causes and technical and behavioral vulnerabilities.

Review events to detect and identify suspicious activities and security violations in order to prioritize them. By having an appropriate history of events, event analysis can be used to correlate events and to better understand circumstances surrounding event occurrences. All these activities support event response, including determining root causes, and actions taken to minimize impacts and better protect the system from suspicious activities and security violations in the future.

CSF Category	CSF Subcategory ID	CSF Subcategory Requirements
Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

Event Analysis

The security-related events should be analyzed to identify and characterize attacks, security compromises, and security incidents. Two primary reasons events are analyzed are:

1. To identify compromises and suspicious conditions, which are often achieved by correlation of related events. This shall include identifying conditions surrounding event

occurrences with attempts to discover root causes, how to handle them, and protect from recurrences.

2. To prioritize or rank them with respect to the risk that they pose.

CSF Category	CSF Subcategory ID	CSF Subcategory Requirements
Anomalies and Events	DE.AE-2	Detected events are analyzed to understand attack targets and methods
	DE.AE-3	Event data are collected and correlated from multiple sources and sensors
	DE.AE-4	Impact of events is determined
Analysis	RS.AN-1	Notifications from detection systems are investigated
	RS.AN-2	The impact of the incident is understood
	RS.AN-3	Forensics are performed
	RS.AN-4	Incidents are categorized consistent with response plans

Incident Handling and Response

An incident response process should be employed and kept current for evaluating and responding to Industrial Automation and Control Systems (IACS) security incidents. A process for evaluating security incidents should be used that identifies the potential impacts and the threats and vulnerabilities that allowed the incident to occur. Evaluation of IACS security incidents allows manufacturers to determine their impact so that an appropriate response can be developed and implemented. Appropriate response should include containment, reducing the impacts, applying counter measures to close the vulnerabilities, and protecting the IACS against future threats.

CSF Category	CSF Subcategory ID	CSF Subcategory Requirements
Information Protection Processes and Procedures	PR.IP-09	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
	PR.IP-10	Response and recovery plans are tested
Communications	RS.CO-1	Personnel know their roles and order of operations when a response is needed
Mitigation	RS.MI-1	Incidents are contained
Response Planning	RS.RP-1	Response plan is executed during or after an incident

Eradication and Recovery

The objective of this phase is to allow the return of normal operations by eliminating artifacts of the incident (e.g., remove malicious code, re-image infected systems) and mitigating the vulnerabilities or other conditions that were exploited. Once the incident is contained, ensure that all means of persistent access into the network have been eradicated, that the adversary activity is sufficiently contained, and that all evidence has been collected. It may also involve hardening or modifying the environment to protect targeted systems and remediating the infected systems. This is often an iterative process. Then restore the impacted systems to operation and verify that it is operating as expected. (Cybersecurity and Infrastructure Security Agency, Cybersecurity Incident & Vulnerability Response Playbooks, Nov. 2021, pp. 15-16. Available: https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf).

Tasks to perform:

Eradication Tasks

1. Remediate all infected systems in the OT environments
2. Reimage affected systems (often from 'gold' sources), or rebuild systems from scratch
3. Rebuild hardware (required when the incident involves rootkits)
4. Install patches
5. Reset passwords on compromised accounts
6. Replace compromised files with clean versions
    a. Download the PLC program
    b. Download the HMI program
    c. Retrieve back up of historian data
7. Monitor for any signs of adversary response to containment activities

Recovery Tasks

1. Tighten perimeter security (e.g., firewall rulesets, boundary router access control lists)
2. Reconnect the rebuilt systems to network
3. Test systems thoroughly, including security controls.
4. Restore systems to normal operations and confirm that they are functioning normally
5. Monitor operations for abnormal behaviors
6. Perform an independent review of compromise and response-related activities.

CSF Category	CSF Subcategory ID	CSF Subcategory Requirements
Recovery Planning	RC.RP-1	Recovery plan is executed during or after a cybersecurity incident

3 Cyber Attack Scenarios

The NIST *Cybersecurity Framework* Respond and Recovery functions will be demonstrated for the following impacts to the plant operation.

1. Loss of View
2. Manipulation of View

3. Loss of Control
4. Manipulation of Control
5. Corrupted program files or data
6. Theft of Operational Information

Cyber threat actors can accomplish these impacts by executing the attack scenarios listed below. We expect that different attacks will require different response and recovery. We are demonstrating capabilities that will address response and recovery from these scenarios

Scenario 1 - Unauthorized Command Message

Adversaries may send unauthorized command messages to instruct control system assets to perform actions outside of their intended functionality. Command messages are used in ICS networks to give direct instructions to control systems devices. If an adversary can send an unauthorized command message to a control system, then it can instruct the control systems device to perform an action outside the normal bounds of the device's actions. An adversary could potentially instruct a control systems device to perform an action that will cause disruption of the manufacturing process or destruction of manufacturing equipment. These maps to the loss of control and manipulation of control impacts in MITRE ATT&CK® for ICS.

Example attacks:

1. In the Dallas Siren incident, adversaries were able to send command messages to activate tornado alarm systems across the city without an impending tornado or other disaster. Alarms were activated more than a dozen times. These disruptions occurred once in 2017, and later in a nearby county in 2019.
2. In the Ukraine 2015 Incident, Sandworm Team issued unauthorized commands to substation breakers after gaining control of operator workstations and accessing a distribution management system (DMS) client application.

Source: [Unauthorized Command Message - attackics (mitre.org)]

Scenario 2 – Modification of Process or Controller Parameters

Adversaries may modify parameters used to instruct industrial control system devices. These devices operate via programs that dictate how and when to perform actions based on such parameters. Such parameters can determine the extent to which an action is performed and may specify additional options. For example, a program on a control system device dictating motor processes may take a parameter defining the total number of seconds to run that motor.

An adversary can potentially modify these parameters to produce an outcome outside of what was intended by the operators. By modifying system and process critical parameters, the adversary may cause Impact to equipment and/or control processes. Modified parameters may be turned into dangerous, out-of-bounds, or unexpected values from typical operations. For example, specifying that a process run for more or less time than it should, or dictating an unusually high, low, or invalid value as a parameter. These maps to the loss of control, manipulation of control, and corrupted program files or data impacts in MITRE ATT&CK® for ICS.

Example attacks:

1. In the Maroochy Attack, Vitek Boden gained remote computer access to the control system and altered data so that whatever function should have occurred at affected pumping stations did not occur or occurred in a different way. The software program

installed in the laptop was one developed by Hunter Watertech for its use in changing configurations in the PDS computers. This ultimately led to 800,000 liters of raw sewage being spilled out into the community.

Source: [Modify Parameter - attackics (mitre.org)]

Scenario 3 – Disabling or Encrypting HMI or Operator Console

Adversaries may cause a denial of view in attempt to disrupt and prevent operator oversight on the status of an ICS environment. This may manifest itself as a temporary communication failure between a device and its control source, where the interface recovers and becomes available once the interference ceases.

An adversary may attempt to deny operator visibility by preventing them from receiving status and reporting messages. Denying this view may temporarily block and prevent operators from noticing a change in state or anomalous behavior. The environment's data and processes may still be operational, but functioning in an unintended or adversarial manner.

Adversaries may cause a sustained or permanent loss of view where the ICS equipment will require local, hands-on operator intervention; for instance, a restart or manual operation. By causing a sustained reporting or visibility loss, the adversary can effectively hide the present state of operations. This loss of view can occur without affecting the physical processes themselves. This maps to the loss of view, manipulation of view, and denial of control impacts in MITRE ATT&CK® for ICS.

Examples:

1. Industroyer is able to block serial COM channels temporarily causing a denial of view.
2. Industroyer's data wiper component removes the registry "image path" throughout the system and overwrites all files, rendering the system unusable.
3. In the Maroochy attack, the adversary was able to temporarily shut an investigator out of the network, preventing them from viewing the state of the system.
4. Some of Norsk Hydro's production systems were impacted by a LockerGoga infection. This resulted in a loss of view which forced the company to switch to manual operations.
5. In the 2017 Dallas Siren incident operators were unable to disable the false alarms from the Office of Emergency Management headquarters.

Source:

[Denial of Control - attackics (mitre.org)]

[Denial of View - attackics (mitre.org)]

Scenario 4 – Data Historian Compromise

Adversaries may compromise the corporate LAN through a phishing email which allows them to gain access to a corporate workstation. Adversaries can utilize this corporate workstation to obtain additional credentials to pivot into the Data Historian in the industrial DMZ. At the core of a Data Historian is a database server, such as Microsoft SQL Server. Access to a data historian can be used to exfiltrate its data that can be used to learn about the process, control systems, and operational details. This knowledge can be subsequently used to launch further attacks into the OT systems. In addition, if the data historian is dual homed, then this can be used to pivot into the OT environment from the IT environment.

Example attacks:

1. The threat group Sandworm Team used the Industroyer malware to attack the Ukrainian power grid in December 2016. The adversary gained Initial Access to devices involved with critical process operations through a Microsoft Windows Server 2003 running a SQL Server.

Source: [Data Historian Compromise - attackics (mitre.org)]

Scenario 5 – Unauthorized Connection is Detected.

Adversaries may perform wireless compromise as a method of gaining communications and unauthorized access to a wireless network. Access to a wireless network may be gained through the compromise of a wireless device. Adversaries may also utilize radios and other wireless communication devices on the same frequency as the wireless network. Wireless compromise can be done as an initial access vector from a remote distance. This maps to one of the techniques in MITRE ATT&CK® for ICS to gain initial access to the ICS environment.

Example:

1. In the Maroochy Attack, the adversary disrupted Maroochy Shire's radio-controlled sewage system by driving around with stolen radio equipment and issuing commands with them. Vitek Boden used a two-way radio to communicate with and set the frequencies of Maroochy Shire's repeater stations.
2. A Polish student used a modified TV remote controller to gain access to and control over the Lodz city tram system in Poland. The remote controller device allowed the student to interface with the tram's network to modify track settings and override operator control. The adversary may have accomplished this by aligning the controller to the frequency and amplitude of IR control protocol signals. The controller then enabled initial access to the network, allowing the capture and replay of tram signals.

Source: [Wireless Compromise - attackics (mitre.org)]

Scenario 6 – Unauthorized Device is Detected.

Adversaries may also setup a rogue communications server to leverage control server functions to communicate with outstations. A rogue communications server can be used to send legitimate control messages to other control system devices, affecting processes in unintended ways. It may also be used to disrupt network communications by capturing and receiving the network traffic meant for the actual communication server. Impersonating a communication server may also allow an adversary to avoid detection. This maps to one of the technics in MITRE ATT&CK® for ICS to gain initial access to the ICS environment.

Example:

1. In the Maroochy Attack, Vitek Boden falsified network addresses in order to send false data and instructions to pumping stations.
2. In the case of the 2017 Dallas Siren incident, adversaries used a rogue communication server to send command messages to the 156 distributed sirens across the city, either through a single rogue transmitter with a strong signal, or using many distributed repeaters.

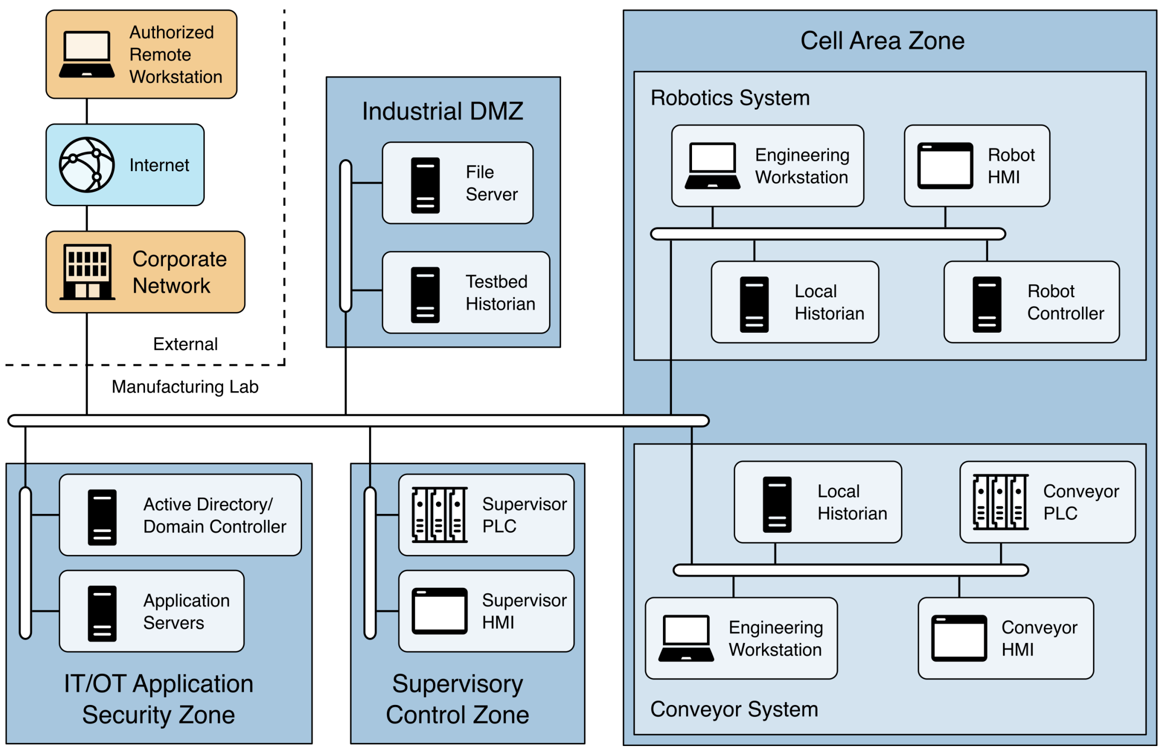
Source: [Rogue Master - attackics (mitre.org)]

404 # 4 Architecture and Capabilities of Lab Environment

405 This section describes the ICS testbed systems in the lab which will be used to demonstrate the
406 cybersecurity capabilities for Response and Recover function.

407 ## Testbed Architecture

408 **Figure 1 High level architecture of the experimentation lab**



409 ### The Process

410 The system is a model manufacturing line consisting of a sorting conveyor system, a robotic arm
411 for parts handling and assembly, and a storage area for finished parts.

412 Three types of parts—bottom, top, and reject—are inserted into an infeed magazine which
413 dispenses them one at a time to the conveyor. On the conveyor, sensors classify the parts to
414 determine if they are a bottom or top piece or a reject piece. Top and bottom pieces are
415 transported to the end station for pickup by the robot. Reject pieces, or out of order top and
416 bottom pieces, are rejected down a chute.

417 The robot retrieves the bottom and top half of a part from the end of the conveyor. The robot
418 places parts on an assembly station. Once both halves arrive, the robot assembles the two parts.
419 Assembled parts are then placed into storage racks. Sensors on the assembly station and in the
420 storage racks verify the presence of parts.

421 Supervisor controls coordinate the two lower level systems.

422 ### Key Control System Components

423 - Conveyor Controls
424   - Programable Logic Controller (PLC)

    - Human Machine Interface (HMI)
- Robot Controls
    - Robot Motion Controller
- Supervisor Controls
    - PLC
    - HMI

Supporting Systems

The systems is supported by engineering workstations that contain the configuration software for the components in the conveyor, robot and supervisory controls.

Windows systems access a central Active Directory (AD) server for authentication and management of accounts. The AD server resides in the Industrial Demilitarized Zone (iDMZ) and is separate from enterprise AD serves.

Overview of Laboratory Capabilities

The lab contains the main components of a manufacturing environment. The systems represent Perdue Model levels zero (0) through three (3) and connections to some higher Perdue level four (4) and five (5) applications.

Servers and workstations are deployed as virtual machines (VMs) with the exception of a physical workstation used as an engineering workstation.

All network switches can have traffic monitored via mirror ports. Open ports are available on physical switches to allow addition of components for security or for scenario execution.

Host-based data can be retrieved from workstations and servers.

Common industrial protocols including OPC, EthernetIP and Profinet are deployed for communication between manufacturing systems.

5 Solution Capabilities and Components

A solution that will provide recovery from an integrity compromise will require a system with multiple capabilities and components. The following system capabilities for an ICS environment are desired:

- Event reporting (Detection)
    - Cyber event detection
        - Network event detection
        - Behavior analysis detection
        - Endpoint detection and response (EDR) (Host based detection)
- Event management
    - Event/Alert notification
    - Case creation
- Log review
    - Collection

    - Aggregation
    - Correlation
- Forensic analysis, In an ICS Environment/on ICS equipment
    - Categorized Incidents based on MITRE ATT&CK for ICS tactics and techniques
    - Understand impact
    - Determination of extent of compromise
- Incident handling and response
    - Containment of the incident
- Eradication of artifacts of incident
- Recovery
    - Restoration of systems
    - Verification of restoration

The system may be composed of the following components or additional components:

- Identity and Authentication System
- Endpoint Detection and Response
- Network Monitoring Tool
- Behavior Anomaly Detection Tool
- Security Information and Event Monitoring System (SIEM)
- Network Policy Engine (PE)
- Firewall (FW)
- Integration Tool for Security Server/PE/FW
- Configuration Management, Back Up, Patch Management System
- Secure Remote Access
- Data Historian
- Cloud Based ICS Capabilities: Data Historian, SCADA, Manufacturing Execution System, Asset Management System

6 Relevant Standards and Guidance

- Department of Homeland Security, Critical Manufacturing Sector Cybersecurity Framework Implementation Guidance, 2015. Available: https://www.cisa.gov/sites/default/files/publications/critical-manufacturingcybersecurity-framework-implementation-guide-2015-508.pdf.
- Executive Order no. 13636, Improving Critical Infrastructure Cybersecurity, DCPD201300091, Feb. 12, 2013. Available: https://www.govinfo.gov/content/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. 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/legacy-files/data-integrity-project-description-final.pdf.
- NIST, Cybersecurity Framework. Available: https://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.
- MITRE ATT&CK® for Industrial Control Systems, https://collaborate.mitre.org/attackics/index.php/Main_Page.

7 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.

Security Capability	CSF Category	CSF Subcategory ID	CSF Subcategory Requirements
Event Reporting	Detection Processes	DE.DP-4	Event detection information is communicated
	Communications	RS.CO-2	Incidents are reported consistent with established criteria
		RS.CO-3	Information is shared consistent with response plans
		RS.CO-4	Coordination with stakeholders occurs consistent with response plans
Log Review	Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and **reviewed** in accordance with policy
Event Analysis	Anomalies and Events	DE.AE-2	Detected events are analyzed to understand attack targets and methods
		DE.AE-3	Event data are collected and correlated from multiple sources and sensors
		DE.AE-4	Impact of events is determined
	Analysis	RS.AN-1	Notifications from detection systems are investigated
		RS.AN-2	The impact of the incident is understood
		RS.AN-3	Forensics are performed
		RS.AN-4	Incidents are categorized consistent with response plans
Incident handling response	Information Protection Processes and Procedures	PR.IP-09	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
		PR.IP-10	Response and recovery plans are tested
	Communications	RS.CO-1	Personnel know their roles and order of operations when a response is needed
	Mitigation	RS.MI-1	Incidents are contained
	Response Planning	RS.RP-1	Response plan is executed during or after an incident
Eradication, Recovery	Recovery Planning	RC.RP-1	Recovery plan is executed during or after a cybersecurity incident

Appendix B Acronyms and Abbreviations

CRS	Collaborative Robotics System
DMZ	Demilitarized Zone
CTL	Communication Technology 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
OT	Operational Technology
PCS	Process Control System
PLC	Programmable Logic Controller
SP PR	Special Publication Protect