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
Lynette Wilcox
Kangmin Zheng

The MITRE Corporation
McLean, Virginia

Revision 1

December 2022

manufacturing_nccoe@nist.gov

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 a data integrity incident 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

The Operational Technology (OT) that runs manufacturing environments play a critical role in the supply chain. Manufacturing organizations rely on OT 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, it cannot guarantee elimination of all cyber risks; therefore, manufacturing organizations should also have a plan to recover and restore operations should a cyber incident impact operations. The goal of this project is to demonstrate means to recover equipment from a cyber incident 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 OT attack within the manufacturing sector by leveraging the following cybersecurity capabilities: event reporting, log review, event analysis, and incident handling and response. The NCCoE will map the security characteristics to the NIST *Cybersecurity 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

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

DISCLAIMER

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

Purpose

This document defines a National Cybersecurity Center of Excellence (NCCoE) project focused on responding to and recovering from a cyber incident within an Operational Technology (OT) environment. Manufacturing organizations rely on OT to monitor and control physical processes that produce goods for public consumption. These same systems are facing an increasing number of cyber incidents 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 (e.g., 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* (NIST *Cybersecurity Framework*) Functions and Categories. Multiple systems need to work together to recover equipment and restore operations when data integrity is compromised. This project explores methods to effectively restore corrupted data in 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 incident in an OT 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 incident within an OT 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 (CSF)* Respond and Recover functions and categories are used to guide this project. The objective of the NIST *Cybersecurity Framework* Respond function is to develop and implement the appropriate activities to take action regarding a detected cybersecurity event. The objective of the 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 are systems such as enterprise resource planning (ERP), manufacturing resource planning (MRP), and manufacturing execution systems (MES) that operate on traditional information technology (IT) infrastructures that run on Windows or Linux

operating systems. 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 cyber incident is discovered after some impact has occurred or prior to impact occurring. A cyber incident can be caused by a variety of factors including but not limited to a well-intentioned insider making a change without proper testing, a malicious insider, or an outside adversary. A comprehensive security architecture should be designed to detect cyber incidents prior to impact including detection of initial access, discovery, and lateral movement. However, a comprehensive defense should also be prepared to restore and recover in the event that a cyber incident is not detected until it is too late. This guide focuses on the hopefully rare event of a cyber incident causing an impact.

A cyber incident is any compromise to systems or data confidentiality, integrity, or availability. This could be caused by a malicious outsider gaining access and making changes or stealing data. But this could just as easily, and possibly more likely, be caused by someone just doing their job and making a mistake or failing to fully test changes prior to implementation. For this reason, this project addresses cyber incidents generically without concern of what or who caused the incident. However, some scenarios in this project would only happen due to malicious actions and have, therefore, been described as such.

To make the rest of the document more readable, the term "malicious actor" will be used to encompass everything from a malicious insider, who already has access, to an advanced persistent threat actor, who conducts a long-term targeted campaign against a system. This also includes lower-level outside malicious actors performing attacks such as widespread ransomware campaigns for profit.

The term "non-malicious actor" will be used to indicate an actor who does not have malicious intent but causes a cyber incident. The cyber incident could be a mistake, a change that has unintended consequences or an untested update that causes disruption to normal operations.

This project assumes:

- The lab infrastructure for this project has a relatively small number of robotic and manufacturing process nodes which are representative of a larger manufacturing facility.
- The effectiveness of the example solutions is independent of the scale of the manufacturing environment.
- 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:
    - Managed and protected physical access to the site
    - Segmentation of OT assets from IT assets
    - Authentication and authorization mechanisms for accessing OT assets
    - Fully managed remote access to the OT environment and OT assets

- Asset and vulnerability management
- Continuous monitoring and detection
- IT Network protection measures (such as firewalls, segmentation, intrusion detection, etc.)
- Addressed vulnerabilities associated with the supply chain and vendor access
- People and processes that support back-up and overall enterprise incident response plans.

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. The following challenges associated with backups are acknowledged:

- 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 essential to the nation's economic security. It is critical for manufacturers to consider how cyber incidents could affect plant operations and the safety of people and property. The 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 OT security. The aim is to address 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 OT networks to improve business agility and operational efficiency. However, recent attacks on OT have shown that malicious actors are pivoting into the OT environment from business systems and IT networks. Most OT systems have been historically isolated from business systems and IT networks, and therefore, were not designed to withstand cyber attacks. The cyber risk mitigation technologies used in IT networks are often not suitable for OT networks because of the real-time and deterministic nature of the OT. These lead to the increasing likelihood that organizations may have to respond or recover from an OT cyber incident. This project will provide guidance to manufacturing organizations for designing mitigations into an OT environment to address cyber incidents.

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 incidents in the OT environment.

2 CYBERSECURITY CAPABILITIES TO BE DEMONSTRATED

This project will demonstrate an approach for responding to and recovering from an OT cyber incident within the manufacturing sector. The cybersecurity capabilities listed below are the typical sequential tasks that take 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

A 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 industrial automation and control system (IACS) cybersecurity published by the International Society of Automation (http://www.isa.org).

Executing these capabilities in a systematic way requires appropriate Respond and Recover roles and personnel assigned to these roles. Typical roles employed in a Respond-and-Recover function are listed below. The number of roles and personnel implemented will depend on the size of the organization, type of industry, and budget.

Internal Resources:

1. Operational Technology (OT) and IT Security Operations Center (SOC) Analyst (if SOC is internally managed)
2. Designated Incident Commander
3. Operations leadership
4. Safety personnel
5. On-call OT systems personnel
6. On-call IT personnel
7. Physical security personnel
8. Administrative personnel
9. Procurement personnel
10. Public relations and legal personnel

External Industry Partners:

1. OT and IT SOC Analyst (if SOC is managed by third party)
2. OT technical support (e.g., vendors, integrators)

3. Operational supply chain (e.g., suppliers, customers, distributors, business partners)
4. Incident response team
5. Surge support
6. Impacted community (e.g., facility neighbors)

Event Reporting

Once an event is detected, it should be reported to the appropriate predetermined stakeholders for initial triage. The triage process will assign an appropriate priority for handling the incident. Based on the priority, predetermined administrative processes will be activated to distribute information about the risk to the appropriate personnel for timely follow up actions.

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 activity for reviewing and analyzing events. Retaining event/audit logs provides support for forensics, which allows identification of root causes, technical vulnerabilities, behavioral vulnerabilities, and improvement opportunities.

Reviewing events to detect and identify suspicious activities and security violations in order to prioritize them should occur. With an appropriate history of events, an event analysis can be conducted to correlate events and to better understand circumstances surrounding event occurrences. All of these activities support an event response, including determining root causes and taking actions 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 is often achieved by correlation of related events. This includes identifying conditions surrounding event occurrences with attempts to discover root causes, how to handle them, and protect from recurrences; and,
2. To prioritize and categorize the incident based on the risk 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 OT cyber incidents. A process for evaluating cyber incidents should be used that identifies the potential impacts, threats, and vulnerabilities that allowed the incident to occur. Evaluation of OT security incidents allows manufacturers to determine their impact so that an appropriate response can be developed and implemented. An appropriate response should include containment, reducing the impact, applying counter measures to mitigate root cause, and protecting the OT against future threats.

CSF Category	CSF Subcategory ID	CSF Subcategory Requirements
Information Protection Processes and Procedures	PR.IP-9	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 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, all means of persistent access into the network should be eradicated so that any malicious actor activity is sufficiently limited, 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. The impacted systems should be restored to operation with verification that they are 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 based on organization's policy:

Eradication Tasks

1. Remediate all infected systems in the OT environments
2. Identify and validate the integrity of correct backup before restoration
3. Reimage affected systems or rebuild systems from scratch
4. Rebuild the hardware (required when the incident involves rootkits)
5. Install patches
6. Reset account passwords
7. Replace compromised files with clean versions
    a. Download the PLC program
    b. Download the HMI program
    c. Retrieve back up of historian data
8. Monitor for any signs of malicious actor 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 the 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. Backup the new configuration on a secure media
7. 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 Recover functions will be demonstrated using the following scenarios which could subsequently impact plant operations.

We expect different incidents to require different response and recovery steps and these scenarios provide an opportunity to demonstrate varied capabilities that will address response and recovery.

Scenario 1 - Unauthorized Command Message

A malicious or non-malicious actor may send unauthorized command messages to instruct control system assets to perform actions outside of their intended functionality. Command messages are used in OT networks to give direct instructions to control systems devices. If a malicious actor can send an unauthorized command message to a control system, then it can instruct the control system's device to perform an action outside the normal bounds of the device's actions. The malicious actor could, therefore, cause disruption of the manufacturing process or destruction of manufacturing equipment.

Potential impact: This maps to the loss of control and manipulation of control impacts listed 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: MITRE ATT&CK® for ICS, T0855. Available:

Unauthorized Command Message, Technique T0855 - ICS | MITRE ATT&CK®

Scenario 2 – Modification of Process or Controller Parameters

A malicious or non-malicious actor 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. Modification of these parameters can produce an outcome outside of what was intended by the operators. By modifying system and process-critical parameters, an actor 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.

Potential impact: This maps to loss of control, manipulation of control, and corrupted program files or data impacts in MITRE ATT&CK® for ICS.

Example attack:

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: MITRE ATT&CK® for ICS, T0836. Available:

Modify Parameter, Technique T0836 - ICS | MITRE ATT&CK®

Scenario 3 – Compromise Human Machine Interface (HMI) or Operator Console

A malicious actor may cause a denial of view in an attempt to disrupt and prevent operator oversight on the status of an OT 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.

A malicious actor 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.

A malicious actor may cause a sustained or permanent loss of view where the OT equipment will require local, hands-on operator intervention; for instance, a restart or manual operation. By causing a sustained reporting or visibility loss, the malicious actor can effectively hide the present state of operations. This loss of view can occur without affecting the physical processes themselves.

Potential impact: This maps to the loss of view, manipulation of view, and denial of control impacts in MITRE ATT&CK® for ICS.

Example attacks:

1. Industroyer was 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: MITRE ATT&CK® for ICS T0813, T0815. Available:

Denial of Control, Technique T0813 - ICS | MITRE ATT&CK®

Denial of View, Technique T0815 - ICS | MITRE ATT&CK®

Scenario 4 – Data Historian Compromise

A malicious actor could gain access to the business network and use this to pivot into the OT environment giving access to the Data Historian. 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 further into the OT environment from the IT environment.

Potential impact: This maps to the collection tactic of Data from Information Repositories in MITRE ATT&CK® for ICS.

Example attack:

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: MITRE ATT&CK® for ICS S0604, T0802. Available:

Industroyer, Software S0604 | MITRE ATT&CK®

Automated Collection, Technique T0802 - ICS | MITRE ATT&CK®

Scenario 5 – Unauthorized Device Detected

A malicious or non-malicious actor may connect an unauthorized device to a wireless network. Access to a wireless network may be gained through a known password being used on an unauthorized device or through a compromise of a wireless device. A malicious actor 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.

Potential impact: This maps to one of the techniques in MITRE ATT&CK® for ICS to gain initial access to the OT environment.

Examples:

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: MITRE ATT&CK® for ICS, T0860. Available:

Wireless Compromise, Technique T0860 - ICS | MITRE ATT&CK®

Scenario 6 – Unauthorized Connection Detected

A malicious actor 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 a malicious actor to avoid detection.

Potential impact: This maps to one of the techniques in MITRE ATT&CK® for ICS to gain initial access to the ICS environment.

Examples:

1. In the Maroochy Attack, Vitek Boden falsified network addresses in order to send spoofed 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: MITRE ATT&CK® for ICS, T0848. Available:

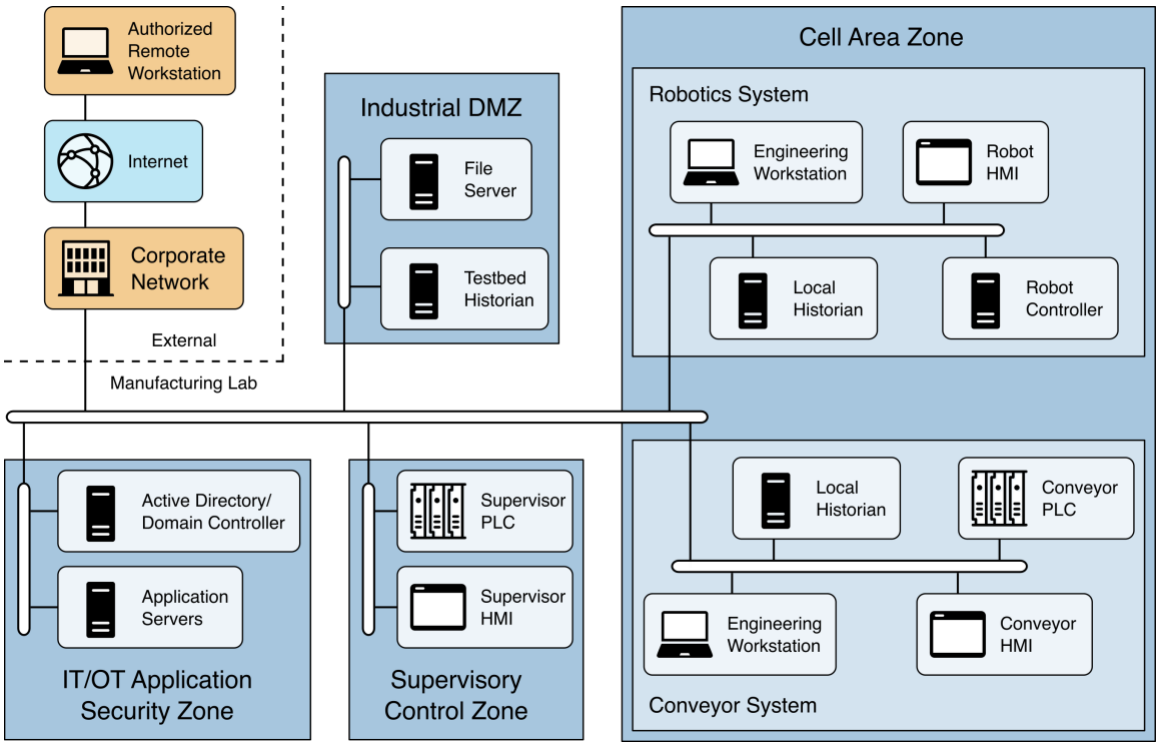
Rogue Master, Technique T0848 - ICS | MITRE ATT&CK®

4 Architecture and Capabilities of Lab Environment

This section describes the OT testbed systems in the lab which will be used to demonstrate the cybersecurity capabilities for Respond and Recover functions.

Testbed Architecture

Figure 1 High level architecture of the experimentation lab



Manufacturing Process

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

Three types of parts (top, bottom, and reject) are inserted into an infeed magazine which dispenses them one at a time to the conveyor. Sensors on the conveyor classify the parts by type. Top and bottom pieces are transported to the end station for pickup by the robot. Reject pieces and out-of-order top and bottom pieces are rejected down a chute.

A robotic arm retrieves the bottom and top halves from the end of the conveyor and places them in an assembly station. Once both halves arrive, the robot assembles the two parts before placing them into storage racks. Sensors on the assembly station and in the storage racks verify the presence of parts.

The Supervisor PLC controls coordinate the two lower-level systems.

Key Control System Components

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

5 SOLUTION CAPABILITIES AND COMPONENTS

The following system capabilities are desired for the OT environment as part of the response and recovery project:

- Event reporting (Detection)
    - Network event detection
    - Behavior anomaly detection
    - Endpoint detection and response (EDR) (Host based detection)
- Event management
    - Event/Alert notification
    - Case creation
- Log review
    - Collection
    - Aggregation
    - Correlation
- Forensic analysis
    - Categorize incidents based on MITRE ATT&CK for ICS tactics and techniques
    - Understand impact
    - Determine root cause
    - Determine extent of compromise
- Incident handling and response
    - Containment of the incident
- Eradication of artifacts of incident
- Recovery
    - Restoration of systems
    - Verification of restoration

To demonstrate the scope specified in this Project Description, the NCCoE is seeking to include the following components:

- Identity and Access Management System
- Endpoint Detection and Response System
- Network Monitoring Tool
- Behavior Anomaly Detection Tool
- Network and Host-based Intrusion Detection Systems
- 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 OT Capabilities: Data Historian, Supervisory Control and Data Acquisition (SCADA), Asset Management System

6 RELEVANT STANDARDS AND GUIDANCE

- Barrett, M. (2018), *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*, *NIST Cybersecurity Framework*, [online], https://doi.org/10.6028/NIST.CSWP.04162018; https://www.nist.gov/cyberframework (Accessed May 31, 2022).
- Department of Homeland Security, *Critical Manufacturing Sector Cybersecurity Framework Implementation Guidance*, 2015. Available: https://www.cisa.gov/uscert/sites/default/files/c3vp/framework_guidance/critical-manufacturing-framework-implementation-guide-2015-508.pdf.
- E. Salfati et al., *Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT)*, NIST Interagency Report (NISTIR) 8428, NIST, Jun. 2022. Available: https://doi.org/10.6028/NIST.IR.8428.
- 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.
- J. McCarthy et al., *Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection*, NIST Interagency Report (NISTIR) 8219, NIST, Nov. 2018. Available: https://doi.org/10.6028/NIST.IR.8219.
- 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.
- T. McBride et al., *Data Integrity: Recovering from Ransomware and Other Destructive Events*, NIST SP 1800-11, Sep. 2020, Available: https://doi.org/10.6028/NIST.SP.1800-11.
- M. Powell et al., *Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector*, NIST SP 1800-10, Mar. 2022, Available: https://doi.org/10.6028/NIST.SP.1800-10.
- 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.
- MITRE ATT&CK® for ICS, https://attack.mitre.org/versions/v11/matrices/ics/.

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 *NIST Cybersecurity Framework*. 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-9	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 A ACRONYMS AND ABBREVIATIONS

AD	Active Directory
AE	Anomalies and Events
AN	Analysis
CO	Communications
CRS	Collaborative Robotics System
CSF	Cybersecurity Framework
CTL	Communication Technology Laboratory
DE	Detect
DP	Detection Process
DMZ	Demilitarized Zone
ERP	Enterprise Resource Planning
FW	Firewall
HMI	Human-Machine Interface
ICS	Industrial Control System(s)
IP	Information Protection Processes and Procedures
IT	Information Technology
MES	Manufacturing Execution Systems
MI	Mitigation
MRP	Manufacturing Resource Planning
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
OT	Operational Technology
PCS	Process Control System
PLC	Programmable Logic Controller
PR	Protect
PT	Protective Technology
RC	Recover
RP	Recovery Planning, Response Planning
RS	Respond
SCADA	Supervisor Control and Data Acquisition
SP	Special Publication