|  |  |
| --- | --- |
|  |  |

ICS/OT Incident Response Program Guide

|  |  |  |
| --- | --- | --- |
| Date | Services Performed By: | Services Performed For: |
| January 23, 2019 |  | Customer XYZ |

# Table of Contents

[Table of Contents 2](#_Toc514315496)

[Executive Summary 2](#_Toc514315497)

[Key References for OT Incident Response Program 5](#_Toc514315498)

[Key Elements of an Incident Response Plan 6](#_Toc514315499)

[Key Questions from DHS ICS-CERT 8](#_Toc514315500)

[Reporting Requirements and Response Support Collaboration 8](#_Toc514315501)

[Defining and Categorizing an Incident 9](#_Toc514315502)

[Hunting Tips 16](#_Toc514315503)

[Attack Indicators 21](#_Toc514315504)

[Jump Kits 23](#_Toc514315505)

[Appendix A: Glossary of Terms 24](#_Toc514315506)

[Appendix B: Additional OT security procedure examples from US DoD CYBERCOM 25](#_Toc514315507)

[B.2. IT/Network Assets 26](#_Toc514315508)

[C.3. Recover – RTU, MTU, and PLC 28](#_Toc514315509)

[C.4. Recover – Intelligent Electronic Devices (IEDs) 29](#_Toc514315510)

[C.5. Recover – Human-Machine Interface (HMI) 30](#_Toc514315511)

[C.7. Recover – Media Converters (Serial/Fiber Converter) 32](#_Toc514315512)

# Executive Summary

To ensure the safe, reliable and continuous operations of your OT assets and manufacturing operations NIST, ICS-CERT, ISA and DoD USCYBERCOM have provided several standards, templates and best practices to enable organizations with OT assets and OT dependent operations to create an incident response program tailored to those OT assets and operations. In the current landscape of espionage from competitors, attacks from nation states and increased knowledge of malicious actors, it is prudent for owners and operators of OT assets to have a defined and tailored incident response program. Organizations should have system, business unit and enterprise level incident response plans that speak to several key areas such as Preparation, Identification, Containment, Eradication, Recovery and Lessons Learned. The incident response plans, policies and procedures should identify roles, responsibilities, reporting chains, points of contact, categories of incidents and events, escalation procedures and steps for troubleshooting and analysis within the system or asset level plans.

**Note: NIST SP 800-53, 82 & 61 and ISA/IEC 62443-3-3:**

**The IR – Incident Response controls family in NIST SP 800-53 defines various sub controls to be considered and tailored within an environment for Incident Response. NIST SP 800-82 provides supplemental guidance for OT environments and NIST SP 800-61 provides a detailed walk through and template for building incident response plans and programs within an organization. Additionally, ISA/IEC 62443-3-3 has baseline recommendations for OT environments found within the FR-6 Timely Response to Events controls.**

# Key References for OT Incident Response Program

The following is a list of authoritative, trusted and experienced references that should be leveraged when any organization seeks to stand up or improve an incident response program for OT operations and assets. These references formed the basis of the recommendations and content within this program guide. In the cases where the reference is more IT centric it must be tailored for OT unique assets and operational environments. In some cases, the OT specific references have already done some tailoring of the IT centric references. Each reference is publicly available online and copies can also be provided upon request.

* SANS Institute – “Incident Handlers Handbook”
* NIST SP 800-61 – “Computer Security Incident Handling Guide”
* NIST SP 800-82 – “Guide to Industrial Control Systems (ICS) Security”
* NIST SP 800-53 – “Security and Privacy Controls for Federal Information Systems and Organizations”
* US Department of Homeland Security (DHS) Industrial Control Systems – Computer Emergency Response Team (ICS-CERT) – “Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability”
* US Department of Defense (DoD) US Cyber Command (USCYBERCOM) – “Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) Industrial Control Systems (ICS)”
* NERC CIP - CIP-008-5 — Cyber Security — Incident Reporting and Response Planning

Additional authoritative and international OT security and safety standards can be obtained from the International Society of Automation (ISA) and the International Electrotechnical Commission (IEC). The key standards for OT security are within the ISA 99/IEC 62443 standards family. For OT safety standards, the ANSI/ISA 84, IEC 61508 and IEC 61511 standards are the international authoritative sources. ISA and IEC standards are available to the public online but they require a fee for purchase.

|  |  |
| --- | --- |
| **ALERT**   | It is the recommendation of the US intelligence community as well as OT security organizations and experts within government and industry that all OT environments implement a layered security approach. This includes environments that are properly air gapped and segmented from the corporate IT environment. Threat actors have evolved in a post Stuxnet world and post nation-state overt doctrine world to take a layered attack approach to critical infrastructure with an increased focus on and knowledge of OT. Security monitoring, security assessments and security engineering integration into brownfield and greenfield projects and operations are recommended best practices. This includes ensuring that integrators, contractors and vendors are implementing security best practices during the lifecycle of existing and new OT assets and operations. |

# Key Elements of an Incident Response Plan

|  |  |
| --- | --- |
| **PREPARE** | Create policies, plans and procedures that form the Incident Response program. Creating the program should define the team, roles and responsibilities, access control, tools and training, reporting and escalation requirements, classification of incidents, templates to be used, the program strategy and communications plans. This should include how the incident response team will interact with internal stakeholders and external stakeholders such as the press, managed security service providers, impacted customers and government entities. |
| **IDENTIFY** | Identify what normal operations looks like. Determine and document what tags, set points, function codes, objects, properties, commands, registers and coils are set within each type of OT device and system. Enforce this requirement within all contracts and all OT operations policy and procedures. Determine which forms and modes of communication all OT assets use and by which protocols they communicate. The identify phase should then focus on deviations from authorized practices within each OT environment. Create an OT call group so that OT operators can report unexpected, unusual and unauthorized changes to a generally static and real-time OT system, device, communications conduit and or protocol. Track and document which OT device, system, physical asset, logic process or program and human user has deviated from expected norms. Catalog false positives for future analysis for at least six months in case that information becomes related to a true incident in later phases of the incident response lifecycle. |
| **CONTAIN** | When unauthorized, unexpected and unusual behavior is detected within a OT asset, device, system or network, steps must be taken to isolate where possible to avoid disruption of critical OT operations. In OT this phase has a different meaning than it does in IT. In IT you can disable devices and pull nodes off the network. In OT you cannot unplug or disable a field controller receiving inputs and sending outputs to control critical real-time operating physical assets. In OT ensure that program logic backups are maintained, tested and deployable. Create a spare parts inventory with applicable operational program logic on standby. If possible only implement protocols and modular devices that can be programmed, simulated and downloaded to the controller without major disruption to operations. This allows OT operators to alter the logic of the compromised I/O module or terminal and activate the logic in a spare I/O terminal block. Additionally, alter OT firewall filters and data connections through your unidirectional gateways or data diodes to close non-essential possible pivot points. An example would be close the communication path into the DMZ where a data historian server could be located and alter the OT device program logic and communications to prevent a compromised controller from speaking to other controllers on the network where possible. |
| **ERADICATE** | Where possible swap out compromised devices during an emergency maintenance window with tested clean devices, loaded with the applicable program logic. Analyze the compromised asset, device, system and network segments for signs of persistent adversaries. Where applicable patch OT workstations and devices in coordination with the vendor and integrator to ensure patching won’t do the job of disruption for the adversary. In OT environments patching is not always the immediate or correct solution to mitigating a potential vulnerability. Work with experienced OT engineers, vendors, programmers and OT focused security experts to determine proper eradication actions for the specific protocol, communications conduit, application, system and device in question at the time. |
| **RECOVER** | When analysis of infected OT assets is complete you should continue to test them in a non-production mode. It is also recommended to leverage these machines for incident response and forensics training as well as development, validation and testing environments where possible. Additionally, consider using these devices as clean swappable spares in future incidents. Schedule a maintenance window based on level of urgency and impact to OT operations to return the cleaned assets back to their production state. |
| **LESSONS LEARNED** | Once you’ve recovered from the incident it is good to document a play by play of the Who, What, When, Where, Why and How. This documentation should tell the story of the incident in such a way that the incident can be replayed for investigative purposes but also be used as a training tool in preparation for future incidents. Additionally, this document can be used to measure the maturity level for your incident response program and help you have visibility into your blind spots and weaknesses. Who detected the incident? What was the detected behavior? When was it first detected? Where was it detected? Why were certain actions taken or not taken? How did the incident occur and how was it resolved? These are some of the questions that must be captured in lessons learned. For OT specifically, you want to know what vendor device, which protocols, what communications medium, which plant, which user accounts, when was it escalated, who escalated it, who responded, were their integrators or contractors involved and was it an insider threat, what was the impact to life safety and environmental operations etcetera. |

# Key Questions from DHS ICS-CERT

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| •  •  •  •  •  • | What components were affected—type, manufacturer, etc.?  What operating systems, including embedded ones, were affected?  How access was gained?  What damage was done and what potential damage could have been done?  What network  vulnerabilities, if any, allowed access to the ICS?  What standards and technical solutions might have prevented the incident? | •  •  •  •  • | What procedures and policies might have prevented the incident?  What training is necessary to prevent additional exploits?  How was the incident detected, and could it have been found earlier or prevented?  Are we still vulnerable and for how long?  Have vendors provided any patches or other solutions, and if so, were they implemented in the ICS in a timely manner? | •  •  •  • | What were the breakdowns in the incident response, including equipment, communications, lines of authority, vendor interactions, analysis, decision-making and recovery?  What areas need to be improved and have processes changed?  Can this information be shared with trusted partners?  Can this information be shared with appropriate government agencies, including response teams? |  |
|  |  |  |  |  |  |

# Reporting Requirements and Response Support Collaboration

Various International, Federal, State, County, Tribal, Local or sector specific organizations may have required reporting requirements for all physical and cybersecurity incidents. Even when an asset owner does not have any legal or regulatory binding reporting requirements it is good practice, especially within the US, to report all OT related events and incidents to the ICS-CERT within DHS. It is the responsibility of the ICS-CERT to respond to and support all critical infrastructure sector asset owners and operators to protect the use homeland critical sectors with impact to our national economy, life safety, property and national security. Information on how to report an OT incident to ICS-CERT can be found here <https://ics-cert.us-cert.gov/Report-Incident>. Additionally, several of the critical infrastructure sectors identified by DHS have a sector specific Information Sharing and Analysis Center known as an ISAC. The list of critical infrastructure sectors as defined by DHS can be found here <https://www.dhs.gov/critical-infrastructure-sectors>. The list of registered and active ISACs can be located here <https://www.nationalisacs.org/member-isacs>. If your sector does not have an ISAC it is recommended that you work with your sector peers and DHS to create an ISAC, join an ISAC from a sector you are most interdependent with and or join the Multi-State ISAC known as MS-ISAC. Additionally, some states and regions of the US have fusion centers that contain joint task forces with local, state and federal resources such as law enforcement, national guard units with cyber protection teams (CPT) and access to several ISACs as well as interfaces directly to the DHS National Cybersecurity and Communications Integration Center (NCCIC) and ICS-CERT. Establishing those relationships during the Prepare phase of your OT IR program is vital to the success of your collaboration with each entity when an incident occurs.

# Defining and Categorizing an Incident

Within an incident response program, during the preparation phase of the incident response lifecycle, each organization must define types, classes and levels of events. This includes defining when an event becomes an incident and then further defining types, classes, categories and escalation levels for incidents. Doing this in the preparation phase and ensuring it is well documented, communicated and trained in the preparation phase ensures that organizations are much more prepared for events and incidents as they occur. OT security best practices from authoritative sources such as ICS-CERT and DoD and standards from NIST can help guide asset owners and operators in defining incident categories.

* NIST SP 800-82 states that “various types of ICS incidents should be identified and classified as to potential impact so that a proper response can be formulated for each potential incident.”
* NIST SP 800-61 defines an event as “any observable occurrence in a system or network”. An incident is defined as “a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices”.

Examples of incidents in OT could be unauthorized and or unexpected values within function codes and commands.

|  |  |
| --- | --- |
| **Incident Response Security Controls**:  The following tables provide more information on incident response security controls from NIST and ISA. Remember that security controls should be analyzed, assessed and tailored to each device, system, network and operational environment not blindly or blanket applied across the entire OT asset and operations footprint. |  |
|  |

|  |  |  |
| --- | --- | --- |
| **NIST SP 800-53 rev4 & 82 rev 2 Incident Response Security Controls** | | |
| **Control ID** | **Control Name** | **REQUIREMENTS** |
| IR-1 | INCIDENT RESPONSE POLICY AND PROCEDURES | The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and b. Reviews and updates the current: 1. Incident response policy [Assignment: organization-defined frequency]; and 2. Incident response procedures [Assignment: organization-defined frequency]. |
| IR-2 | INCIDENT RESPONSE TRAINING | The organization provides incident response training to information system users consistent with assigned roles and responsibilities: a. Within [Assignment: organization-defined period] of assuming an incident response role or responsibility; b. When required by information system changes; and c. [Assignment: organization-defined frequency] thereafter.  **Control Enhancements:** (1) INCIDENT RESPONSE TRAINING | SIMULATED EVENTS The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations. (2) INCIDENT RESPONSE TRAINING | AUTOMATED TRAINING ENVIRONMENTS The organization employs automated mechanisms to provide a more thorough and realistic incident response training environment. |
| IR-3 | INCIDENT RESPONSE TESTING | The organization tests the incident response capability for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the incident response effectiveness and documents the results.  **Control Enhancements:** (1) INCIDENT RESPONSE TESTING | AUTOMATED TESTING The organization employs automated mechanisms to more thoroughly and effectively test the incident response capability. (2) INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS The organization coordinates incident response testing with organizational elements responsible for related plans. |
| IR-4 | INCIDENT HANDLING | The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.  **Control Enhancements:** (1) INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES The organization employs automated mechanisms to support the incident handling process. (2) INCIDENT HANDLING | DYNAMIC RECONFIGURATION The organization includes dynamic reconfiguration of [Assignment: organization-defined information system components] as part of the incident response capability. (3) INCIDENT HANDLING | CONTINUITY OF OPERATIONS The organization identifies [Assignment: organization-defined classes of incidents] and [Assignment: organization-defined actions to take in response to classes of incidents] to ensure continuation of organizational missions and business functions. (4) INCIDENT HANDLING | INFORMATION CORRELATION The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response. (5) INCIDENT HANDLING | AUTOMATIC DISABLING OF INFORMATION SYSTEM The organization implements a configurable capability to automatically disable the information system if [Assignment: organization-defined security violations] are detected. (6) INCIDENT HANDLING | INSIDER THREATS - SPECIFIC CAPABILITIES The organization implements incident handling capability for insider threats. (7) INCIDENT HANDLING | INSIDER THREATS - INTRA-ORGANIZATION COORDINATION The organization coordinates incident handling capability for insider threats across [Assignment: organization-defined components or elements of the organization]. (8) INCIDENT HANDLING | CORRELATION WITH EXTERNAL ORGANIZATIONS The organization coordinates with [Assignment: organization-defined external organizations] to correlate and share [Assignment: organization-defined incident information] to achieve a cross organization perspective on incident awareness and more effective incident responses. (9) INCIDENT HANDLING | DYNAMIC RESPONSE CAPABILITY The organization employs [Assignment: organization-defined dynamic response capabilities] to effectively respond to security incidents. (10) INCIDENT HANDLING | SUPPLY CHAIN COORDINATION The organization coordinates incident handling activities involving supply chain events with other organizations involved in the supply chain. |
| IR-5 | INCIDENT MONITORING | The organization tracks and documents information system security incidents.  **Control Enhancements:** (1) INCIDENT MONITORING | AUTOMATED TRACKING / DATA COLLECTION / ANALYSIS The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information. |
| IR-6 | INCIDENT REPORTING | The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within [Assignment: organization-defined time]; and b. Reports security incident information to [Assignment: organization-defined authorities].  **Control Enhancements:** (1) INCIDENT REPORTING | AUTOMATED REPORTING The organization employs automated mechanisms to assist in the reporting of security incidents. (2) INCIDENT REPORTING | VULNERABILITIES RELATED TO INCIDENTS The organization reports information system vulnerabilities associated with reported security incidents to [Assignment: organization-defined personnel or roles]. (3) INCIDENT REPORTING | COORDINATION WITH SUPPLY CHAIN The organization provides security incident information to other organizations involved in the supply chain for information systems or information system components related to the incident. |
| IR-7 | INCIDENT RESPONSE ASSISTANCE | The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.  **Control Enhancements**: (1) INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT The organization employs automated mechanisms to increase the availability of incident response related information and support. (2) INCIDENT RESPONSE ASSISTANCE | COORDINATION WITH EXTERNAL PROVIDERS The organization: (a) Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and (b) Identifies organizational incident response team members to the external providers. |
| IR-8 | INCIDENT RESPONSE PLAN | The organization: a. Develops an incident response plan that:  1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and 8. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; b. Distributes copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; c. Reviews the incident response plan [Assignment: organization-defined frequency]; d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; e. Communicates incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and f. Protects the incident response plan from unauthorized disclosure and modification. |
| IR-9 | INFORMATION SPILLAGE RESPONSE | The organization responds to information spills by: a. Identifying the specific information involved in the information system contamination; b. Alerting [Assignment: organization-defined personnel or roles] of the information spill using a method of communication not associated with the spill; c. Isolating the contaminated information system or system component; d. Eradicating the information from the contaminated information system or component; e. Identifying other information systems or system components that may have been subsequently contaminated; and f. Performing other [Assignment: organization-defined actions].  **Control Enhancements:** (1) INFORMATION SPILLAGE RESPONSE | RESPONSIBLE PERSONNEL The organization assigns [Assignment: organization-defined personnel or roles] with responsibility for responding to information spills. (2) INFORMATION SPILLAGE RESPONSE | TRAINING The organization provides information spillage response training [Assignment: organization defined frequency]. (3) INFORMATION SPILLAGE RESPONSE | POST-SPILL OPERATIONS The organization implements [Assignment: organization-defined procedures] to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions. (4) INFORMATION SPILLAGE RESPONSE | EXPOSURE TO UNAUTHORIZED PERSONNEL The organization employs [Assignment: organization-defined security safeguards] for personnel exposed to information not within assigned access authorizations. |
| IR-10 | INTEGRATED INFORMATION SECURITY ANALYSIS TEAM | The organization establishes an integrated team of forensic/malicious code analysts, tool developers, and real-time operations personnel. |

|  |  |  |  |
| --- | --- | --- | --- |
| **ISA 62443-3-3 Functional Requirement (FR)-6 – Timely Response to Events** | | | |
| **Functional Requirements**  **And Systems**  **Requirement**  **ID** | **Functional and System Requirement Name** | **Requirement Purpose and Rational** | **Security Levels (SL) and Requirement Enhancements (RE)** |
| FR-6 | Timely response to events | Respond to security violations by notifying the proper authority, reporting needed evidence of the violation and taking timely corrective action when incidents are discovered.  **Rationale:** Using their risk assessment methodology, asset owners should establish security policies and procedures and proper lines of communication and control needed to respond to security violations. Derived prescriptive recommendations and guidelines should include mechanisms that collect, report, preserve and automatically correlate the forensic evidence to ensure timely corrective action. The use of monitoring tools and techniques should not adversely affect the operational performance of the control system. | SL 1 – Monitor the operation of the IACS and respond to incidents when they are discovered by collecting and providing the forensic evidence when queried.  SL 2 – Monitor the operation of the IACS and respond to incidents when they are discovered by actively collecting and periodically reporting forensic evidence. SL 3 – Monitor the operation of the IACS and respond to incidents when they are discovered by actively collecting and pushing forensic evidence to the proper authority.  SL 4 – Monitor the operation of the IACS and respond to incidents when they are discovered by actively collecting and pushing forensic evidence to the proper authority in near real-time. |
| SR 6.1 | Audit log accessibility | The control system shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.  **Rationale and supplemental guidance:** The control system generates audit records about events occurring in the system (see 6.10, SR 2.8 – Auditable events). Access to these audit logs is necessary to support filtering audit logs, identifying and removing information that is redundant, reviewing and reporting activity during after-the-fact investigations of security incidents. This access should not alter the original audit records. In general, audit reduction and report generation should be performed on a separate information system. Manual access to the audit records (such as screen views or printouts) is sufficient for meeting the base requirement, but is insufficient for higher SLs. Programmatic access is commonly used to provide the audit log information to analysis mechanisms such as SIEM. See relevant SRs in clauses 5, 6 and 9 regarding the creation of, protection of and access to audit logs. | **Requirement enhancements** (1) Programmatic access to audit logs. The control system shall provide programmatic access to audit records using an application programming interface (API).  The requirements for the four SL levels that relate to SR 6.1 – Audit log accessibility are:   SL-C (TRE, control system) 1: SR 6.1  SL-C (TRE, control system) 2: SR 6.1  SL-C (TRE, control system) 3: SR 6.1 (1)   SL-C (TRE, control system) 4: SR 6.1 (1) |
| SR 6.2 | Continuous monitoring | The control system shall provide the capability to continuously monitor all security mechanism performance using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner.  **Rationale and supplemental guidance:** Control system monitoring capability can be achieved through a variety of tools and techniques (for example, IDS, IPS, malicious code protection mechanisms and network monitoring mechanisms). As attacks become more sophisticated, these monitoring tools and techniques will need to become more sophisticated as well, including for example behavior-based IDS/IPS.  Monitoring devices should be strategically deployed within the control system (for example, at selected perimeter locations and near server farms supporting critical applications) to collect essential information. Monitoring mechanisms may also be deployed at ad hoc locations within the control system to track specific transactions.  Monitoring should include appropriate reporting mechanisms to allow for a timely response to events. To keep the reporting focused and the amount of reported information to a level that can be processed by the recipients, mechanisms such as SIEM are commonly applied to correlate individual events into aggregate reports which establish a larger context in which the raw events occurred.  Additionally, these mechanisms can be used to track the effect of security changes to the control system (see 6.10, SR 2.8 – Auditable events). Having forensic tools pre-installed can facilitate incident analysis. | The requirements for the four SL levels that relate to SR 6.2 – Continuous monitoring are:   SL-C (TRE, control system) 1: Not Selected   SL-C (TRE, control system) 2: SR 6.2   SL-C (TRE, control system) 3: SR 6.2  SL-C (TRE, control system) 4: SR 6.2 |

# Hunting Tips

Many of the incident response practices from IT security can be carried over into some of the OT operational practices and the higher layers of an OT architecture. However, there are some hunting techniques and troubleshooting tips that need to be kept in mind as unique to the types of embedded computing devices that OT devices consist of. Below are examples of OT device troubleshooting and analysis techniques that should be completed to determine if an OT device is encountering an unexpected malfunction and or a malicious incident. These examples are from the US DoD CYBERCOM “Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) Industrial Control Systems (ICS)” Appendix.

|  |  |  |  |
| --- | --- | --- | --- |
|  | | **A.1.1–EVENT DIAGNOSTICS** |  |
| **SECTION** | **EVENT** | **DESCRIPTION** | **PAGE** |
| **FIELD DEVICE ANOMALIES** | |  |  |
| A.2.17 | Abnormal Decrease in  Control Process Traffic or  Loss of Communications | The normal flow of control traffic appears slower, sluggish, or there is less traffic than normal (polling cycles not executing for example). | A-22 |
| A.2.18 | Unusual Field Device  Activity Observed/  Reported | Any anomalous behavior coming from field devices could be hardware malfunctions or communication path malfunctions. However, once these have been ruled out, a cyber incident should be considered as the possible source of the problem. | A-23 |
| A.2.19 | Unexpected Changes to Ladder Logic/Code Configurations, Firmware, and Set Points | Changes to the controller logic within the field device could come from a process that has been altered, a new process that has been implemented, an old process that was removed, or a process that was hijacked. | A-24 |
| A.2.20 | HMI, OPC, or Control Server  Sending False Information | If false information is sent to the control system, it could either be an error, or a malicious attempt to disguise unauthorized changes or an initiation of inappropriate actions by system operators. | A-25 |
| A.2.21 | Anomalous Safety Systems  Modifications | Anomalous modifications to the safety system could come from an error in the system, accidental misconfiguration, or some other explained event. If the change to the safety system cannot be explained, the changes could be malicious with the intention of damaging the control system. | A-26 |

|  |  |
| --- | --- |
| **A.2.17–FIELD DEVICE: ABNORMAL DECREASE IN CONTROL PROCESS TRAFFIC OR LOSS OF COMMUNICATIONS** | |
| * **Functional Area**: IT or ICS * **Description**: The normal flow of control traffic appears slower, sluggish, or there is less traffic than normal (for example, polling cycles not executing) | |
| **STEP** | **PROCEDURES** |
| **Investigation** | 1. **DETERMINE** if an authorized activity or hardware/software malfunction is the cause for the decrease in control traffic:    * Did a batch process execute?    * Is a device malfunctioning?    * Did a service stop running? 2. If a failure occurred within the ICS equipment, **CONDUCT** regular trouble shooting activities. |
| **No Action**  **Required** | 3. If the anomaly can be explained by a malfunction or authorized activity:   * **DOCUMENT** the **Severity Level as None** (0) in the Security Log. * **CONTINUE** with the next diagnostic procedure. If all applicable procedures have been completed, **RETURN** to Routine Monitoring. |
| **If Action**  **Required** | 1. If the anomaly cannot be explained by a malfunction or authorized activity:    * **DOCUMENT** in Security Log.    * **GO TO** Section A.3, A.3.1 Integrity Checks Table. (See recommended checks below). **IDENTIFY** the field device being investigated. **CONDUCT** the integrity checks on the device.   **Recommended Checks:**  A.3.2.9 Controller Integrity Check  A.3.2.11 Firewall Log Review  A.3.2.5 Server/Workstation Unresponsive Check  A.3.2.4 Server/Workstation Communications Check   1. Once you have completed all appropriate Integrity Checks, **GO TO** section **A.2.29 Action Step**. |

|  |  |
| --- | --- |
| **A.2.18–FIELD DEVICE: UNUSUAL FIELD DEVICE ACTIVITY OBSERVED / REPORTED** | |
| * **Functional Area**: IT or ICS * **Description**: Unless field devices are under manual control, field devices should be exhibiting behavior that is synchronized with the commands sent by the OPC or control server or the HMI. Any anomalous behavior coming from field devices could be hardware malfunctions or communication path malfunctions. However, once these have been ruled out, a cyber incident should be considered as the possible source of the problem.   Lack of correlation between measurements  Devices’ settings are not within normal parameters  Abnormal communication between controllers and field devices  Blocked or delayed information passing from controllers to field devices | |
| **STEP** | **PROCEDURES** |
| **Investigation** | **1. DETERMINE** if a hardware or communications failure is causing the anomaly. **CONDUCT** hardware/software trouble-shooting. |
| **No Action**  **Required** | 2. If the anomaly was caused by a hardware or communications failure:   * **DOCUMENT** the **Severity Level as None** (0) in the Security Log. * **CONTINUE** with the next diagnostic procedure. If all applicable procedures have been completed, **RETURN** to Routine Monitoring. |
| **If Action**  **Required** | 1. If the anomaly was not related to a hardware or communications malfunction:    * **DOCUMENT** in Security Log.    * **GO TO** Section A.3, A.3.1 Integrity Checks Table. (See recommended checks below.) **EXECUTE** the integrity checks.   **Recommended Checks:**  A.3.2.9 Controller Integrity Check  A.3.2.1 Server/Workstation Process Check  A.3.2.4 Server/Workstation Communications Check  A.3.2.11 Firewall Log Review   1. Once you have completed all appropriate Integrity Checks, **GO TO** section **A.2.29 Action Step**. |

|  |  |
| --- | --- |
| **A.2.19–FIELD DEVICE: UNEXPECTED CHANGES TO LADDER LOGIC, CODE CONFIGURATIONS, FIRMWARE, AND SET POINTS** | |
| * **Functional Area**: IT or ICS * **Description**: Changes to the controller logic within the field device could come from a process that has been altered, a new process that has been implemented, an old process that was removed, or a process that was sabotaged | |
| **STEP** | **PROCEDURES** |
| **Investigation** | **1. DETERMINE** if the changes in the controller logic were authorized changes. |
| **No Action**  **Required** | 2. If changes to the controller logic were authorized:   * **DOCUMENT** the **Severity Level as None** (0) in the Security Log. * **CONTINUE** with the next diagnostic procedure. If all applicable procedures have been completed, **RETURN** to Routine Monitoring. |
| **If Action**  **Required** | 1. If changes to the controller logic were not authorized:    * **DOCUMENT** in Security Log.    * **IDENTIFY** the devices from which controller logic can be changed.    * **GO TO** Section A.3, A.3.1 Integrity Checks Table. (See recommended checks below.) **LOCATE** the integrity checks associated with these devices, and **EXECUTE** the integrity checks.   **Recommended Checks:**  A.3.2.9 Controller Integrity Check  A.3.2.2 Server/Workstation Log Review (for upstream asset)  A.3.2.1 Server/Workstation Process Check (for upstream asset)   1. Once you have completed all appropriate Integrity Checks, **GO TO** section **A.2.29 Action Step**. |

|  |  |
| --- | --- |
| **A.2.20–FIELD DEVICE: HMI, OPC, OR CONTROL SERVER SENDING FALSE INFORMATION** | |
| * **Functional Area**: IT or ICS * **Description**: If false information is sent to the control system, it could be an error, or a malicious attempt to disguise unauthorized changes, or an initiation of inappropriate actions by system operators | |
| **STEP** | **PROCEDURES** |
| **Investigation** | **1. DETERMINE** if changes to field controller configurations or anomalous commands sent were authorized. |
| **No Action**  **Required** | 2. If changes to the controller logic were authorized:   * **DOCUMENT** the **Severity Level as None** (0) in the Security Log. * **CONTINUE** with the next diagnostic procedure. If all applicable procedures have been completed, **RETURN** to Routine Monitoring. |
| **If Action**  **Required** | 1. If changes to the controller logic were not authorized:    * **DOCUMENT** in Security Log.    * **IDENTIFY** the devices from which controller logic can be changed.    * **GO TO** Section A.3, A.3.1 Integrity Checks Table. (See recommended checks below.) **LOCATE** the integrity checks associated with these devices, and **EXECUTE** the integrity checks.   **Recommended Checks:**  A.3.2.9 Controller Integrity Check  A.3.2.4 Server/Workstation Communications Check  A.3.2.5 Server/Workstation Unresponsive Check  A.3.2.3 Unauthorized User Account Activity  A.3.2.1 Server/Workstation Process Check  A.3.2.13 Server/Workstation Rootkit Check   1. Once you have completed all appropriate Integrity Checks, **GO TO** section **A.2.29 Action Step**. |

|  |  |
| --- | --- |
| **A.2.21–FIELD DEVICE: ANOMALOUS SAFETY SYSTEMS MODIFICATIONS** | |
| * **Functional Area**: IT or ICS * **Description**: Anomalous modifications to the Safety System could come from an error in the system, accidental misconfiguration, or some other explained event. If the change to the Safety System cannot be explained, the changes could be malicious with the intention of damaging the control system. | |
| **STEP** | **PROCEDURES** |
| **Investigation** | **1. DETERMINE** if the changes to the Safety System were authorized. |
| **No Action**  **Required** | 2. If changes to the controller logic were authorized:   * **DOCUMENT** the **Severity Level as None** (0) in the Security Log. * **CONTINUE** with the next diagnostic procedure. If all applicable procedures have been completed, **RETURN** to Routine Monitoring. |
| **If Action**  **Required** | 1. If changes to the controller logic were not authorized:    * **DOCUMENT** in Security Log.    * **IDENTIFY** the devices from which controller logic can be changed.    * **GO TO** Section A.3, A.3.1 Integrity Checks Table. (See recommended checks below.) **LOCATE** the integrity checks associated with these devices, and **EXECUTE** the integrity checks.   **Recommended Checks:**  A.3.2.9 Controller Integrity Check   1. Once you have completed all appropriate Integrity Checks, **GO TO** section **A.2.29 Action Step**. |
| **END OF FIELD DEVICE ANOMALIES** | |

# Attack Indicators

Every mature and effective incident response program focuses on key attack indicators to focus the scope of monitoring, analysis, alerting and response on areas most likely to be signs of malicious and unauthorized activity. Making these indicators part of your incident response operations can also help to decrease the focus on potential noise and false positives saving your incident response team valuable time by helping them focus on the essentials. Below are some key indications of attacks in OT environments as recommended by ICS-CERT and taken from NIST SP 800-82 “Guide to Industrial Control Systems (ICS) Security”:

* Unusually heavy network traffic
* Out of disk space or significantly reduced free disk space
* Unusually high CPU usage
* Creation of new user accounts
* Attempted or actual use of administrator-level accounts
* Locked-out accounts
* Accounts in use when the user is not at work
* Cleared log files
* Full log files with an unusually large number of events
* Antivirus or IDS alerts
* Disabled antivirus software and other security controls
* Unexpected patch changes
* Machines or intelligent field devices connecting to outside Internet Protocol (IP) addresses
* Requests for information about the system (social engineering attempts)
* Unexpected changes in configuration settings
* Unexpected system shutdown
* Stoppage or displayed error messages on a web, database, or application server
* Unusually slow access to hosts on the network
* Filenames containing unusual characters or new or unexpected files and directories
* Auditing configuration changes logged on the host records, especially disabling of auditing functionality
* A large number of bounced e-mails with suspicious content
* Unusual deviation from typical network traffic flows
* Erratic ICS equipment behavior, especially when more than one device exhibits the same behavior
* Any apparent override of safety, backup, or failover systems
* Equipment, servers, or network traffic that has bursts of temporary high usage when the operational process itself is steady and predictable.
* Unknown or unusual traffic from corporate or other networks external to control systems network
* Unknown or unexpected firmware pulls or pushes.

# Jump Kits

It is paramount that jump kits be created during the preparation phase and updated during every new introduction of an OT product or upgrade and or significant change to exist devices especially backups of program logic. Some OT vendors and integrators have strict licensing requirements so it is imperative for OT operators and asset owners to ensure backups of license dongles and license files are kept up to date within the OT jump kits at each site. Jump kits must be located on site or at least capable of quickly arriving through express shipping and or flyaway response teams. Below is a list of contents that mature jump kits should contain for OT environments per USCYBERCOM:

* Incident Notifications List: document contact information for Cybersecurity Managers and OT Security Managers
* Document stakeholders who could be affected by a Cyber-attack on OT
* Establish notification procedures with chain of command
* Operational Security Logs
* IT and OT system schematics
* Universal serial bus (USB) drives, bootable USB (or LiveCD) with up-to-date anti-malware, and other software tools that can read and/or write to file system (Example: Bart’s PE disk)
* Laptop with anti-malware utilities and Internet access (for downloads)
* Computer and network tool kit to add/remove components, hard drives, connectors, wire cables, etc.
* Hard disk duplicators with write-block capabilities to capture hard drive images
* Firewall access control lists
* Firewall hard disk image
* IDS rules
* IDS image
* Back up of IT and OT firewall, router, and switch OS
* Backup of PLC configurations and firmware
* Backup RTU software, database, and configurations
* Back up of all other computer assets to include HMI, Historian, and Database
* Network map of all expected connections to the OT
* Bootable rescue CD with tools, rootkit detection, master boot record check, and other capabilities

**Example Operational Security Log**

Date

:

6/15/

16

Operator

:

Joe Operator

**Time**

**Asset**

**IP Address**

**Description**

**Actions Taken**

**Results**

830

Primary HMI

10.10.10.14

Event Log Review

Examined Event

Logs

Six failed log-on

attempts

845

OPC Server

10.10.10.12

User Accounts

Reviewed user

accounts

Escalated

privileges on user

accounts

900

Notification

Contacted ISSM

and provided

information on

activity

ISSM

recommends

moving to

Mitigation

915

Primary HMI, OPC

Server

10.10.10.14

,

10.10.10.12

Started Mitigation

Disconnected

Ethernet cable

from port 6 on

SCADA Switch

Network segment

is separated from

the network

**Figure 1:**

Operational Security Log Example from US DoD USCYBERCOM

|  |  |
| --- | --- |
|  | Air gapped OT assets and regulatory compliance alone will not protect critical operations from security threats. In recent years security threats have become multifaceted and persistent. Additionally, nation states are no longer the sole entities capable of carrying out such multi-stage attacks. Many organizations lack the budget and persistent resources on the OT operations side to deploy a dedicated always on OT security platform combined with dedicated services such as security engineering, security monitoring and analysis operations as well as security assessments of assets and sites. Outsourced staff augmentation is an experienced practice for IT, but is very much needed in OT to face down the new evolving threats in today’s political and economic climate. |

# Appendix A: Glossary of Terms

* CPT – USCYBERCOM Cyber Protection Teams
* FMC – Fully Mission Capable
* ICS – Industrial Control Systems (also known as OT)
* ISSE – Information Systems Security Engineer
* ISSM – Information Systems Security Manager
* ISSO – Information Systems Security Officer

# Appendix B: Additional OT security procedure examples from US DoD CYBERCOM

|  |  |
| --- | --- |
| **A.3.2.9 CONTROLLER INTEGRITY CHECK** | |
| * **Who should do this check**: The organization or individual responsible for the integrity of field controllers * **What is needed for this check**:   1. FMC field controller configuration files   2. FMC baseline topology   3. Field controller vendor documentation   4. Jump-Kit | |
| **STEP** | **PROCEDURES** |
| 1 | If the controller contains log files, **REVIEW** the log files for anomalies. |
| 2 | **USE** Jump-Kit as appropriate. |
| 3 | **COMPARE** state of field device with field controller settings. May include:   * **CHECK** to see if Mode is correct. * **CHECK** lights and indicators. |
| 4 | Connect the Jump-Kit computer to the device. |
| 5 | If possible, **RETRIEVE** the field controllers FMC configuration files. If **not possible, GO TO** Step 10. |
| 6 | **EXTRACT** configuration files from field controller. |
| 7 | **COMPARE** extracted configuration file to FMC configuration file. |
| 8 | If the values match and there is no change in the mode, and the log files do not contain anomalies:   * **DOCUMENT** the **Severity Level as None** (0). * **EXIT** procedure, **RETURN** to the originating diagnostic procedure and continue with Recommended Checks. |
| 9 | If the values do not match, **DOCUMENT** in the Security Log. |
| 10 | On the baseline topology, IDENTIFY which HMI is communicating with the field controller. |
| 11 | **CONTACT** the operator of that HMI, and brief operator on status of controller. |
| 12 | **REQUEST** the HMI operator **COMPARE** the configuration settings recorded in the HMI with those of the field controller. |
| 13 | **DOCUMENT** HMI operator’s response in Security Log. |
| 14 | **RECOMMEND** HMI operator review the HMI application (whether the values between the controller match). |
| 15 | **VALIDATE** the set points and operating condition of the field device connected to the field controller. |
| 16 | If an anomaly is identified from the previous steps:   * **DOCUMENT** details of the event in the Security Log. * **DOCUMENT** the **Severity Level of High (3)**. * **GO TO** section **A.2.29 Action Step**. |
| 17 | If anomaly does not exist:   * **DOCUMENT** the **Severity Level as None (0)** * **RETURN** to the originating diagnostic procedure and continue with Recommended Checks. |

## B.2. IT/Network Assets

Utilize the IT/Network Device Mitigation Procedure when the affected device(s) discovered during Detection is not directly connected to, or controlling, the ICS process (typical equipment such as switches, routers, firewalls, servers, and workstations).

The main goal of the IT/Network Assets Mitigation is to isolate the infected assets and maintain operation and control of the critical ICS process(es).

|  |  |
| --- | --- |
| **IT/NETWORK DEVICE MITIGATION** | |
| * **Who should perform this procedure**: The organization or individual who has knowledge of the network configuration and the impact on the ICS end process * **What is needed for this procedure**: FMC baseline topology | |
| **STEP** | **PROCEDURES** |
| 1 | When possible, **MAINTAIN POWER** to the affected devices during this procedure. This will aid in after-incident forensic analysis of the cyber event. |
| 2 | When possible, and unless otherwise directed, **PRESERVE** forensic data on the affected device(s). Technical assistance may be required to save the data. For details see Enclosure G: Data Collection for Forensics. |
| 3 | **DOCUMENT** all actions taken in the Security Log for after-incident analysis. |
| 4 | If installed, **SWITCH** control to the secondary or redundant control network, and **MONITOR** the operation of the ICS process(es) to ensure the alternate control network is operating properly. If the secondary or redundant control network is functioning properly, **PROCEED** to the Recovery Procedures in enclosure C for the affected network. If the secondary or redundant control network is not operating properly, **PROCEED** to the ICS Control Device Mitigation Procedure, enclosure B, section B.3. Otherwise, **CONTINUE** with the next step. |
| 5 | If no secondary or redundant control network is installed, **DISCONNECT** the network cable(s) connected to the affected device(s). |
| 6 | After **DISCONNECTING** the network cable(s) on the affected device(s), closely **MONITOR** the operation of the ICS process(es) to ensure that there are no adverse effects indicated. If any adverse effects are indicated, **PROCEED** to the ICS Control Device Mitigation Procedure, enclosure B, section B.3. Otherwise, **CONTINUE** to the next step. |
| 7 | **CONTACT** the ISSM to provide notification that the device has been isolated. |
| 8 | **PROCEED** to the Recovery Procedures in enclosure C. |

## C.3. Recover – RTU, MTU, and PLC

|  |  |
| --- | --- |
|  | **TYPICAL EQUIPMENT: RTU/MTU/PLC** |
| **•** | **Who should perform this procedure**: The organization or individual who has knowledge of the network configuration and the impact on the ICS end process |
| **•** | **What is needed for this procedure**: FMC baseline topology, Jump-Kit |
| **STEP** | **PROCEDURES** |
| 1 | **RECORD** all steps taken while performing these procedures. These records are a requirement of CJCSM 6510-01B and will be utilized for forensic analysis of the cyber incident. |
| 2 | **MAINTAIN** primary power (if possible) to the RTU/MTU/PLC until an image can be saved of the device’s memory. **SAVE** an image of the configuration software and volatile memory (if possible and unless otherwise directed) for forensic analysis. |
| 3 | **REMOVE AND REPLACE** the affected RTU/MTU/PLC. Device replacement will preserve forensic evidence of the cyber incident for analysis. |
| 4 | **DO NOT REIMAGE** any devices unless authorized by the ISSM. Reimaging the affected RTU/MTU/PLC will destroy forensic evidence of the cyber incident. If a replacement RTU/MTU/PLC or modules are not available, **REIMAGE** the affected RTU/MTU/  PLC software/firmware from a trusted, known good source. |
| 5 | **VERIFY** the latest vendor software/firmware patches are installed on the RTU/MTU/PLC. **INSTALL** updates as required. |
| 6 | **UPDATE** passwords on RTU/MTU/PLC. **UTILIZE** robust passwords. |
| 7 | **CONFIRM/UPDATE** the RTU/MTU/PLC set points and configuration files. |
| 8 | **TEST** the operation of the RTU/MTU/PLC and the endpoint device(s) while in local operating mode and while still isolated from the wider network (when operating conditions allow). |
|  | **Reintegration** |
| 9 | **DO NOT RECONNECT** the RTU/MTU/PLC to other network devices in the affected network until each device in the network layer or sub-system has been recovered per these procedures. |
| 10 | **VERIFY** that each device in the isolated layer or sub-system has been properly recovered. **CONSULT** the cyber incident records, the ISSM, or CPT to confirm that Recovery has been performed on these devices. |
| 11 | When each device in the sub-system or layer has been recovered, **RECONNECT** all the devices in the sub-system or layer. **DO NOT RECONNECT** to the wider network at this time. |
| 12 | **VERIFY** that the cyber incident artifacts have been eliminated using available Detection tools (IDS, NMap, Netstat, Wireshark, etc). |
| 13 | **MONITOR** the system for anomalous behavior. If anomalous behavior is evident, **RETURN** to the Detection Procedures (enclosure A) and/or Mitigation Procedures (enclosure B) of this ACI TTP as necessary. |
| 14 | When the layer or sub-system is operating without evidence of the cyber incident, and approval is given by the ISSM or CPT, **RECONNECT** the isolated layer or sub-system to the rest of the network. |
| 15 | **MONITOR** the system for anomalous behavior. If anomalous behavior is evident, **RETURN** to the Detection Procedures (enclosure A) and/or Mitigation Procedures (enclosure B) of this ACI TTP as necessary. |
| 16 | **SAVE** an image of the new firmware/configuration hash. |
| 17 | **RETURN** to Routine Monitoring of the network. |
| 18 | **SUBMIT** all records of Recovery actions to the ISSM or CPT. |

## C.4. Recover – Intelligent Electronic Devices (IEDs)

|  |  |
| --- | --- |
| **TYPICAL EQUIPMENT: IEDS; PROTECTIVE RELAY CONTROLLERS, TAP CHANGER CONTROLLERS, CIRCUIT BREAKER CONTROLLERS, CAPACITOR BANK SWITCHES, SWITCH RE-CLOSER CONTROLLERS, VOLTAGE REGULATORS, ETC.** | |
| * **Who should perform this procedure**: The organization or individual who has knowledge of the network configuration and the operation of the ICS end process * **What is needed for this procedure**: FMC baseline topology, Jump-Kit | |
| **STEP** | **PROCEDURES** |
| 1 | **RECORD** all steps taken while performing these procedures. These records are a requirement of CJCSM 6510-01B and will be utilized for forensic analysis of the cyber incident. |
| 2 | **MAINTAIN** primary power (if possible) to the IED until an image can be saved of the device’s memory. **SAVE** an image of the configuration software and volatile memory (if possible and unless otherwise directed) for forensic analysis. |
| 3 | **REMOVE AND REPLACE** the affected IED. Device replacement will preserve forensic evidence of the cyber incident for analysis. |
| 4 | **DO NOT REIMAGE** any devices unless authorized by the ISSM. Reimaging the affected IED will destroy forensic evidence of the cyber incident. If a replacement IED or modules are not available, **REIMAGE** the affected IED software/firmware from a trusted, known good source. |
| 5 | **VERIFY** the latest vendor software/firmware patches are installed on the IED. **INSTALL** updates as required. |
| 6 | **UPDATE** passwords on IED. **UTILIZE** robust passwords. |
| 7 | **SELECT** the optional selectable IP range instead of the default IP. |
| 8 | **CONFIRM/UPDATE** the IED set points and configuration files. |
| 9 | **SAVE** an image of the new firmware/configuration hash. |
| 10 | **TEST** the operation of the IED and the endpoint device(s) while in local operating mode and while still isolated from the wider network (when operating conditions allow). |
| **Reintegration** | |
| 11 | **DO NOT RECONNECT** the IED to other network devices in the affected network until each device in the network layer or subsystem has been recovered per these procedures. |
| 12 | **VERIFY** that each device in the isolated layer or sub-system has been properly recovered. **CONSULT** the cyber incident records, the ISSM, or CPT to confirm that Recovery has been performed on these devices. |
| 13 | When each device in the sub-system or layer has been recovered, **RECONNECT** all the devices in the sub-system or layer. **DO NOT RECONNECT** to the wider network at this time. |
| 14 | **VERIFY** that the cyber incident artifacts have been eliminated using available Detection tools (IDS, NMap, Netstat, Wireshark, etc). |
| 15 | **MONITOR** the system for anomalous behavior. If anomalous behavior is evident, **RETURN** to the Detection Procedures (enclosure A) and/or Mitigation Procedures (enclosure B) of this ACI TTP as necessary. |
| 16 | When the layer or sub-system is operating without evidence of the cyber incident, and approval is given by the ISSM or CPT, **RECONNECT** the isolated layer or sub-system to the rest of the network. |
| 17 | **MONITOR** the system for anomalous behavior. If anomalous behavior is evident, **RETURN** to the Detection Procedures (enclosure A) and/or Mitigation Procedures (enclosure B) of this ACI TTP as necessary. |
| 18 | **SAVE** an image of the new firmware/configuration hash. |
| 19 | **SUBMIT** all records of Recovery actions to the ISSM or CPT. |
| 20 | **RETURN** to Routine Monitoring of the network. |

## C.5. Recover – Human-Machine Interface (HMI)

|  |  |
| --- | --- |
|  | **TYPICAL EQUIPMENT: HUMAN-MACHINE INTERFACE (HMI)** |
| **•** | **Who should perform this procedure**: The organization or individual who has knowledge of the network configuration and the operation of the ICS end process |
| **•** | **What is needed for this procedure**: FMC baseline topology, Jump-Kit |
| **STEP** | **PROCEDURES** |
| 1 | **RECORD** all steps taken while performing these procedures. These records are a requirement of CJCSM 6510-01B and will be utilized for forensic analysis of the cyber incident. |
| 2 | **MAINTAIN** primary power (if possible) to the HMI until an image can be saved of the device’s memory. **SAVE** an image of the configuration software and volatile memory (if possible and unless otherwise directed) for forensic analysis. |
| 3 | **REMOVE AND REPLACE** the affected HMI. Device replacement will preserve forensic evidence of the cyber incident for analysis. |
| 4 | If a replacement HMI is not available, **REMOVE AND REPLACE** the hard drive (if installed) with a back-up drive containing software from a trusted, known good source. |
| 5 | **DO NOT REIMAGE** any devices unless authorized by the ISSM or CPT. Reimaging the affected HMI will destroy forensic evidence of the cyber incident. If a replacement HMI or hard drive not available, **REIMAGE** the affected HMI software/firmware from a trusted, known good source. |
| 6 | Rootkit infections/detections will require **REFLASHING** of the BIOS on the server/workstation. An example of generic BIOS reflash procedure follows. Check your vendor documentation for specific instructions for your device. Before you REFLASH the BIOS:   * **DISABLE** BIOS Flash Protection in the BIOS setup. * **VERIFY** the BIOS version update is the correct BIOS for your machine. * Do not interrupt the BIOS when updating; improper BIOS flashing will result in system malfunctions. * When the BIOS **REFLASH** is complete, **ENABLE** BIOS Flash Protection in the BIOS setup menu. |
| 7 | **VERIFY** the latest vendor software/firmware patches are installed on the HMI. **INSTALL** updates as required. |
| 8 | **UPDATE** passwords on HMI. **UTILIZE** robust passwords. |
| 9 | **VERIFY** that system configurations are correctly displayed on the HMI. |
| 10 | **UPDATE** the antivirus software (if installed) with the latest update, and INITIATE a full system scan. |
|  | **Reintegration** |
| 11 | **DO NOT RECONNECT** the HMI to other network devices in the affected network until each device in the network layer or subsystem has been recovered per these procedures. |
| 12 | **VERIFY** that each device in the isolated layer or sub-system has been properly recovered. Consult the cyber incident records, the ISSM, or CPT to confirm that Recovery has been performed on these devices.   * **RECONNECT** the device or sub-system. * **DO NOT RECONNECT** to the wider network at this time. |
| 13 | **VERIFY** that the cyber incident artifacts have been eliminated using available Detection tools (IDS, NMap, Netstat, Wireshark, etc). |
| 14 | **MONITOR** the system for anomalous behavior. If anomalous behavior is evident, **RETURN** to the Detection Procedures (enclosure A) and/or Mitigation Procedures (enclosure B) of this ACI TTP as necessary. |
| 15 | **VERIFY** that changes in system indications are accurately indicating on the HMI, and the HMI has proper control over the system. |
| 16 | When the layer or sub-system is operating without evidence of the cyber incident and approval is given by the ISSM or CPT, **RECONNECT** the isolated layer or sub-system to the rest of the network. |
| 17 | **MONITOR** the system for anomalous behavior. If anomalous behavior is evident, **RETURN** to the Detection Procedures (enclosure A) and/or Mitigation Procedures (enclosure B) of this ACI TTP as necessary. |
| 19 | **SUBMIT** all records of Recovery actions to the ISSM or CPT. |
| 20 | **RETURN** to Routine Monitoring of the network. |

## C.7. Recover – Media Converters (Serial/Fiber Converter)

systems and will focus on preservation of forensic evidence of the cyber incident for analysis.

|  |  |
| --- | --- |
|  | **TYPICAL EQUIPMENT: MEDIA CONVERTERS (SERIAL TO FIBER, SERIAL TO ETHERNET)** |
| **•** | **Who should perform this procedure**: The organization or individual who has knowledge of the network configuration and the operation of the ICS end process |
| **•** | **What is needed for this procedure**: FMC baseline topology, Jump-Kit |
| **STEP** | **PROCEDURES** |
| 1 | **RECORD** all steps taken while performing these procedures. These records are a requirement of CJCSM 6510-01B and will be utilized for forensic analysis of the cyber incident. |
| 2 | **REMOVE AND REPLACE** the affected converter. |
| 3 | If the converter contains firmware and a replacement is not available, **REFLASH** the firmware from a trusted source. |
|  | **Reintegration** |
| 4 | **DO NOT reconnect** devices or network layers until each component has been functionally tested and all attributes of the cyber incident have been eliminated. |
| 5 | **VERIFY** that each device in the isolated layer or sub-system has been properly recovered. **CONSULT** the cyber incident records, the ISSM, or CPT to confirm that Recovery has been performed on these devices.   * **RECONNECT** the device or sub-system. * **DO NOT** reconnect to the wider network at this time. |
| 6 | **VERIFY** that the cyber incident artifacts have been eliminated using available Detection tools (IDS, Log Review, NMap, Netstat, Wireshark, etc). |
| 7 | **MONITOR** the system for anomalous behavior. If anomalous behavior is evident, **RETURN** to the Detection Procedures (enclosure A) and/or Mitigation Procedures (enclosure B) of this ACI TTP as necessary. |
| 8 | When the layer or sub-system is operating without evidence of the cyber incident and approval is given by the ISSM or CPT, **RECONNECT** the isolated layer or sub-system to the rest of the network. |
| 9 | **MONITOR** the system for anomalous behavior. If anomalous behavior is evident, **RETURN** to the Detection Procedures (enclosure A) and/or Mitigation Procedures (enclosure B) of this ACI TTP as necessary. |
| 10 | **SUBMIT** all records of Recovery actions to the ISSM or CPT. |
| 11 | **RETURN** to Routine Monitoring of the network. |