RECLAMATION MANUAL RELEASE

Comments on this draft release must be submitted to proreliability@usbr.gov by 02/23/2026.

Facilities Instructions Standards and Techniques (FIST) Manual 3-33 Operational Technology Systems - Supervisory Control and Data Acquisition and Electronic Access Control and Surveillance System Systems Operation and Maintenance

This document represents a comprehensive rewrite of FIST 3-33. The updated version was developed by a Reclamation Implementation Team composed of Subject Matter Experts (SMEs) from each regional office.

Rationale for Revision Outdated Source Material:
The original FIST 3-33 was published in 2013, based on the guidance and regulations available at that time. Since then, nearly all referenced documents have undergone significant updates, necessitating a complete revision. Inclusion of EACSS: Electronic Access Control and Surveillance Systems (EACSS) have been added to FIST 3-33 as part of its coverage of Operational Technology (OT) systems.

Integration of PEB 59: The 2016 publication of PEB 59, Maintenance Schedule for Security and Surveillance Systems, introduced numerous updated tasks relevant to OT systems. Key information from PEB 59 has been incorporated into the revised FIST 3-33, allowing PEB 59 to be retired.

BUREAU OF RECLAMATION

Facilities Instructions, Standards, and Techniques - Volume 3-33

Operational Technology Systems - Supervisory Control and Data Acquisition and Electronic Access Control and Surveillance System Systems Operation and Maintenance

Mission Statements

The U.S. Department of the Interior protects and manages the Nation's natural resources and cultural heritage; provides scientific and other information about those resources; honors its trust responsibilities or special commitments to American Indians, Alaska Natives, Native Hawaiians, and affiliated Island Communities.

The mission of the Bureau of Reclamation is to manage, develop, and protect water and related resources in an environmentally and economically sound manner in the interest of the American public.

Disclaimer

This written material consists of general information for internal use only by Bureau of Reclamation operations and maintenance staff. Information contained in this document regarding commercial products or firms may not be used for advertising or promotional purposes and is not to be construed as an endorsement or depreciation of any product or firm by the Bureau of Reclamation.

Cover Photo – Operations Technology Systems (Bureau of Reclamation).

Facilities Instructions, Standards, and Techniques - Volume 3-33

Operational Technology Systems - Supervisory Control and Data Acquisition and Electronic Access Control and Surveillance System Systems Operation and Maintenance

Prepared by

Bureau of Reclamation
Power Resources Office and Regional Team
Denver, Colorado

Contents

Appendices

Record of Revisions

Revision Number	**Date** (Mon/Year)	**Type** (New, Major, Minor, Admin.)	**Reclamation Manual Number and Details**
1.0	XX/XXXX	Major	FIST 3-33 Complete Rewrite. Changed system name to Operational Technology (OT) and added SCADA, EACSS and the Appendix A.

Reclamation Standards and Documents

Reclamation OT systems should be developed to open published standards. This means that any vendor can manufacture products conforming to these standards and will make the selection of products used in OT systems more competitive. In general, try to avoid purchasing OT system components that adhere to proprietary standards.

ANSI/ISA-95	*Enterprise-Control System Integration*
ANSI/ISA-62443	*Industrial Automation and Control Systems Security*
NIST SP 800-82	*ICS security guidance*
NIST SP 800	*Guide to Operational Technology (OT) 3 Security*
NIST FIPS 200	*Minimum Security Requirements for Federal Information and Information System*
FIPS 201/HSPD-12	*Identity verification and access control*
CIP-003	*Cyber Security – Security Management Controls*
CIP-004	*Cyber Security – Personnel & Training*
CIP-005	*Cyber Security – Electronic Security Perimeter(s)*
CIP-006	*Cyber Security – Physical Security of BES Cyber Systems*
CIP-007	*Cyber Security – Systems Security Management*
CIP-008	*Cyber Security – Incident Reporting and Response Planning*
CIP-009	*Cyber Security – Recovery Plans for BES Cyber Systems*
CIP-010	*Cyber Security – Configuration Change Management and Vulnerability Assessments*
CIP-011	*Cyber Security – Information Protection*
CIP-012	*Cyber Security – Communications between Control Centers*
CIP-013	*Cyber Security – Supply Chain Risk Management*
FIST 4-1B	*Maintenance Schedules for Electrical Equipment*
HSPD-12	*Homeland Security Presidential Directive-12*
NARA	*National Archive and Records Administration, General Records Schedule 5.6: Security Management Records.*
NDAA	*2019 John S. McCain National Defense Authorization Act*
SLE 03-02	*Facility Security*
SLE 02-01	*Identifying and Safeguarding Controlled Unclassified Information (CUI)*
RCD 03-03	*Request for Deviation from a Reclamation Manual Requirement and Approval or Disapproval of the Request*

Acronyms and Abbreviations

A list of abbreviations and acronyms used by Operational Technology (OT) system support staff is provided in this appendix. Abbreviations include both industry standard abbreviations and abbreviations that apply to the Bureau of Reclamation Industrial Control Systems (ICS).

ACS	Access Control System
A/D	Analog-to-Digital
AGC	Automatic Generation Control
AI	Analog Input
AO	Analog Output
ASCII	American Standard Code for Information Interchange
ASP	Automatic Synchronization Program
ASR	Automatic Send-Receive
AVC	Automatic Voltage Control
AVM	Acoustic Velocity Meter
BCD	Binary Coded Decimal
BES	Bulk Electric System
BITSM	Reclamation's Information Technology Security Manager
BMS	Balanced Magnetic Switch
BPA	Bonneville Power Administration
BPS	Bits Per Second
BYTE	Eight Bits
CARMA	Capital Asset and Resource Management Application
C&A	Certification and Accreditation
CIP	Critical Infrastructure Protection
COTS	Commercial Off-The-Shelf
CPU	Central Processing Unit
DCS	Distributed Controls Systems
DI	Digital Input
DO	Digital Output
DVR/NVR	Digital/Network Video Recorders
EACSS	Electronic Access Control and Surveillance System
EIA	Electronic Industries Association
EMI	Electromagnetic Interference
EPROM	Erasable Programmable Read-Only Memory
ESS	Electronic Security System

FAT	Factory Acceptance Test
FEP	Front-End Processor
FISMA	Federal Information Security Modernization Act of 2014
FIST	Facilities Instructions, Standards, and Techniques
HMI	Human-Machine Interface
IC	Integrated Circuit
ICS	Industrial Control Systems
IDS	Intrusion Detection System
I/O	Input/Output
IRO	Information Resources Office
IT	Information Technology
K	Kilo
kV	Kilovolt
LCD	Liquid Crystal Display
LED	Light-Emitting-Diode
LSI	Large Scale Integration
MMI	Man-machine Interface
MS	Master Station
ms	Millisecond
MSB	Most Significant Bit
MSD	Most Significant Digit
MTBF	Mean Time Before Failure
MTTR	Mean Time to Repair
MVAR	Megavar
MVR	Megavar
MW	Megawatt
MWh	Megawatthour
NCI	National Critical Infrastructure
NPFA	National Fire Protection Association
NEMA	National Electrical Manufacturer's Association
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
O&M	Operations and Maintenance
OMB	Office of Management and Budget
OSHA	Occupational Safety and Health Administration
OT	Operational Technology
PACS	Physical Access Control System
PCB	Power Circuit Breaker

PIN	Personal Identification Number
P/G	Pump/Generating
PLC	Programmable Logic Controller
PMSC	Programmable Master Supervisory Control
POA&M	Plan of Action and Milestones
PRO&M	Power Review of O&M
RAM	Random Access Memory
Reclamation	Bureau of Reclamation
REMMS	Reclamation Enterprise Maintenance Management System
ROM	Read-Only Memory
RPM	Revolutions Per Minute
RTD	Resistance Temperature Detector
RTU	Remote Terminal Unit
S/A	Synchro-to-Analog
S/D	Synchro-to-Digital
SCADA	Supervisory Control and Data Acquisition
SCP	Synchronization Check Program
SNL	Speed No Load
SOE	Sequence of Event
SOP	Standing Operating Procedures
SSP	System Security Plan
SSPP	System Security and Privacy Plan
TD	Transducer
UAS	Unmanned Aircraft System
UPS	Uninterruptible Power Supply
UTC	Universal Time Code
VSS	Video Surveillance Systems
Western	Western Area Power Administration (WAPA)

1.0 Introduction

The Bureau of Reclamation (Reclamation) operates and maintains hydroelectric powerplants, switchyards, pumping plants, water delivery equipment and associated facilities in the 17 western United States. These facilities house complex electrical and mechanical equipment that must be kept operational because they are critical to the electric power and water delivery systems relied on by many. Facilities Instructions, Standards, and Techniques (FIST) are technical documents that provide criteria and procedures that should be utilized by the offices involved in managing maintenance of Reclamation facilities and assets.

This document establishes standard technical practices to ensure the safe, reliable, economic and efficient Operations and Maintenance (O&M) of Federal facilities by keeping related assets in good condition and ultimately protecting Federal investments. These technical practices provide a sufficient level of detail to ensure consistent application while providing flexibility for the use of innovative techniques and approaches. This document was developed with input from staff in Reclamation's Denver, regional, and area offices.

For equipment not covered in this FIST, please reference online documentation, original manufacturer's documentation, or contractor's installation documentation. If a valid procedure still cannot be found, contact the OT system manager for further guidance.

1.1 Purpose and Scope

This document is intended to promote uniformity in the manner that assets are managed, documented, and coordinated, and may be utilized by transferred facilities and other entities as appropriate. It establishes consistent procedures, minimum standards and O&M criteria for hydroelectric equipment and systems owned and operated by Reclamation. Other technical documents may provide additional electrical and mechanical maintenance information for the equipment or systems discussed in this document.

O&M requirements are based on industry standards and experience. Maintenance requirements vary based on equipment condition and past performance, and sound engineering practices and maintenance management should be employed for special circumstances. Manufacturer recommendations and instructions should be consulted for additional maintenance that may be required beyond what is stated in this manual.

This volume includes standards, practices, procedures, and advice on day-to-day operation, maintenance, and testing of Operational Technology (OT) equipment in Reclamation facilities.

In this document, the term "OT" includes "SCADA systems", "EACSS" and "DCS" etc. This guidance is for both operations personnel that use OT system equipment and support personnel

that maintain OT system equipment. For the purposes of this document, the OT system includes all equipment within the boundary defined in the Authority to Operate (ATO) and all connected peripheral devices (analog and digital).

Reclamation OT systems are diverse in size, complexity, technology, and architecture. FIST Volume 3-33, Operational Technology (OT) Systems, addresses basic practices that provide a standard framework for the periodic review and improvement of OT system O&M programs. This FIST addresses Reclamation OT system O&M practices as follows:

- Addresses operating and maintaining Reclamation OT systems used to protect, control/monitor Reclamation-owned power equipment such as powerplants, pumping plants, switchyards, and other related power facilities. It will not address OT systems that operate Reclamation facilities that are not owned by Reclamation.
- Does not cover the specific operational requirements for the water and electrical power systems controlled and monitored using an OT system. Refer to the Standard Operating Procedures (SOP) or technical equipment manuals for the site to obtain this information.
- Describes some basic training requirements for operators. However, more detailed training requirements that relate to OT system operations are addressed and reviewed from an operations perspective in other documents (see FIST Volume 1-2). It is important to ensure OT system operators have the skills necessary to operate the OT systems used to control their facilities.
- Describes some basic training requirements for system maintainers. However, more detailed training requirements that relate to OT system maintenance are addressed and reviewed from a maintenance perspective in other documents (see FIST Volume 4-1b). It is important to ensure OT system maintainers have the skills necessary to maintain the OT system used to protect and control their facilities.

Note: This document is not a reference for physical, Informational Technology (IT), or any other regulatory security requirements that apply to Reclamation OT systems. It is important to consider security requirements during all phases of an OT system life cycle. However, no effort will be made to cover specific security requirements within this document.

1.2 Reclamation Standard Practices

FIST manuals are designed to provide guidance for maintenance and testing on equipment in Reclamation's facilities. There may be multiple ways to accomplish tasks outlined in this document. Facilities may exercise discretion as to how to accomplish certain tasks based on equipment configurations and available resources.

Reclamation's regions, Power Resources Office (PRO), and Technical Services Center (TSC) agree that certain practices are required to be consistent across all Reclamation facilities. Mandatory FIST procedures, practices, and schedules that appear in **{Red, bold, and bracketed}** or **[Black, bold, and bracketed]** text are considered Reclamation requirements for the O&M of equipment in power facilities. RM D&S FAC 04-14, *Power Facilities Technical Documents*, describes the responsibilities required by text designations: **{Red, bold, and bracketed}**, **[Black, bold, and bracketed]**, and plain text, within this technical document.

Refer to RM D&S FAC 04-14 for more details concerning technical documents.

1.3 Maintenance Tables

Maintenance tables for tasks described in this document are included in FIST 4-1B, Maintenance Scheduling for Electrical Equipment.

1.4 Manufacturer Recommendations

The information in this document is based on manufacturers' documentation and historic Reclamation practices. Due to the differences in equipment designs, owner's manuals and manufacturer's recommended maintenance should be consulted when developing job plans. Not following the manufacturer's guidance may void the warranty of new equipment. If there is a discrepancy between the FIST and the manufacturer's recommendations, the job plan must use the more stringent practice unless there is a reason that a less restrictive maintenance practice is warranted. Use of a less restrictive maintenance practice must be approved as outlined in RM D&S FAC 04-14 by either a deviation or a variance. A deviation maybe granted in accordance with RCD 03-03 and POM Form 300.

1.5 FIST Revision Requests

The FIST Revision Request Form (POM-226) is used to request changes to a FIST document. The request will include a summary of the recommended changes and a basis for the revision or new FIST. These forms will be submitted to the Manager, PRO. The PRO Manager will keep a list of Revision Requests for each FIST and include these in the next scheduled revision unless the change is prioritized sooner.

1.6 Safety During Maintenance Activities

Safety is an essential part of OT maintenance. Identifying the hazards involved with working on or near excitation systems is essential to create a safe working condition.

Personnel performing maintenance on OT systems may involve work on rotating machinery, various types (i.e. ac and dc) and voltage potentials of electricity. Equipment may have high arc flash hazards and potential for stored energy requiring extra care and knowledge. It is important that all hazards be assessed prior to the start of work. All maintenance activities must be conducted in accordance with FIST Volume 1-1, Hazardous Energy Control Program (HECP), FIST Volume 5-14, Electrical Safety Program, and the Reclamation Safety and Health Standards (RSHS). A job hazard analysis (JHA) must be conducted as well.

All actions required to establish an electrically safe work environment must be conducted in accordance with Facilities Instructions, Standards, and Techniques (FIST) 1-1, Hazardous Energy Control Program; FIST 5-14, Electrical Safety Program; and the applicable Facility Hazardous Energy Control Program (F-HECP). Due to the unique conditions found in electronic equipment, a hazard analysis must be conducted utilizing the requirements defined in NFPA 70E for safety related work practices associated when working on Power Electronic equipment. The equipment technical documents must be utilized to ensure any internal hazards due to stored electrical energy from capacitive discharge or other forms of radio frequency energy are identified. Follow all safety requirements established by the equipment manufacturer prior to removing any covers or performing work on any electronic equipment. *Follow all applicable safety procedures*.

2.0 Operational Technology Overview

Operational Technology is defined by the National Institute of Standards and Technology (NIST) as programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms. These OT systems have evolved from early, dedicated systems based almost entirely on custom, proprietary hardware and software to modern network-based systems comprised of Commercial Off-The-Shelf (COTS) hardware and operating systems, which support a mixture of COTS and custom-developed software. Our ongoing facility modernization programs have resulted in using new technologies that increase the level of automation and expand equipment-monitoring capabilities.

Reclamation has used Operational Technology (OT), which includes Supervisory Control and Data Acquisition (SCADA) systems, Distributed Controls Systems (DCS), and Electronic Access Control and Surveillance System (EACSS), for more than 35 years to protect, monitor/control water, and power operations at our dams, canals, pumping plants, powerplants, and other related facilities. Reclamation currently operates and maintains several OT systems identified within this FIST (EACSS and SCADA). For this document, the holistic security system will be referred to as the EACSS and may also be referred to as a Physical Access

Control System (PACS) within Reclamation. The EACSS is comprised of two subsystems, the Electronic Security Systems (ESS) and the Video Surveillance Systems (VSS).

The ESS provides access control and intrusion detection at the facility. Various ESS management software and hardware (e.g., Lenel, AMAG, Bosch, Software House, etc.) is installed at Reclamation facilities. The ESS integrates various sensors, identified below, into a cohesive system which provides for monitoring alarms, auditing access, and reporting status. The ESS is comprised of two major components: the Access Control System (ACS) and the Intrusion Detection System (IDS):

- The ACS grants, revokes, and monitors access throughout the facility, using devices such as card readers and electronic strikes.
- The IDS detects access into the facility, using sensors such as Balanced Magnetic Switch (BMS), motion detectors, and radars.

The VSS provides detection and assessment capability, as well as video archiving of intrusion events. This is achieved using fixed cameras, pan-tilt-zoom (PTZ) cameras, thermal cameras, and digital/network video recorders (DVR/NVR).

Equipment will be compliant with Homeland Security Presidential Directive 12 (HSPD-12), Federal Information Processing Standards (FIPS), the Trade Agreement Act (TAA) and the John S. McCain National Defense Authorization Act (NDAA), section 889. Access control system will not connect to the Federal Bridge. The access control system will be configured for dual authentication using employee Personal Identity Verification (PIV) badge and Personal Identification Number (PIN).

OT systems refer to programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms. Some Reclamation OT systems do not perform any control functions but are dedicated to collecting data. Other remote independent systems require system operators to supervise actual equipment control.

Primarily, OT systems software includes all software for remote and local automated equipment control and for collecting and processing data to directly support control functions. In addition, the OT systems software facilitates data collection and control as required by external entities such as Western Area Power Administration (Western or WAPA), Bonneville Power Administration (BPA), other Federal agencies, other interconnected system operating authorities, local irrigation districts, and local power customers. OT systems software typically includes:

1. Real-time data acquisition software
2. Report generation software

3. Real-time unit and plant control software
4. Standard control software (logic controls, feedback controls)
5. Database software
6. Communication software
7. Human-machine interface (HMI) software for the display of real-time, alarm, and trend-data and for the control of the units and plant
8. A variety of software development tools and system configuration tools
9. Remote Terminal Unit (RTU)
10. Programmable Logic Controller (PLC)

For each OT system, it will be important to determine the boundary of the OT system. Typically, historical archiving, maintenance management, and water scheduling functions are not considered part of the OT system. As plants begin to install intelligent devices at the local equipment level, the RTU functions are being distributed among a set of computerized devices that are no longer purchased as part of the plant OT system.

The boundary for the OT system should include all equipment within the boundary used for OT system Assessment and Authorization (A&A) which is required for authority to operate by Reclamation. This boundary can include a diversity of equipment depending on the network configuration but is ultimately defined in the System Security Plan (SSP) as stipulated by the A&A. Note that the local intelligent devices are subject to similar requirements as the OT system itself. They require many of the same safeguards to ensure proper operation and maintenance goals are achieved.

3.0 Security

All Reclamation OT systems are subject to the requirements contained in the Office of Management and Budget (OMB) Circular A-130 (Appendix III, as amended) and the Federal Information Security Management Act (FISMA) of 2002 (44 United States Code Section (§) 3541). Beginning with the passage of the Energy Policy Act of 2005, new Federal cyber security requirements became effective. These new requirements, identified in the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards, are directly applicable to a subset of Reclamation cyber systems, where those systems specifically support Bulk Electric System (BES) reliability. OT system security requirements are critical to protect, operate, and maintain Reclamation OT systems properly. The primary goal of OT

systems security reviews is to protect the OT systems rather than to address system proper operation and maintenance.

Information technology security requirements for OT systems are addressed through implementing Federal requirements as directed and interpreted by Reclamation's Information Resources Office. Standards have been developed for a variety of security controls, including both physical security and cyber security requirements. Some of the key requirements include those published by:

1. NIST – Specifically, Special Publication 800-53 addressing the security of Federal information technology systems.

2. The Federal Information Security Modernization Act of 2014 (FISMA 2014) updates the Federal Government's cybersecurity practices. The FISMA 2014 codifies the Department of Homeland Security's role in administering the implementation of information security policies for federal Executive Branch civilian agencies, overseeing agencies' compliance with those policies, and assisting OMB in developing those policies.

3. The NERC CIP Reliability Standards while applicable to many OT systems, primarily are intended to address security requirements of OT systems controlling power facilities identified as NERC Facilities.

It should be noted that these security standards (apart from the NERC Standards) typically focus on requirements for administrative IT systems and their applications. Applying these requirements to the security of OT systems and applications is to be done carefully so as not to compromise the operational usefulness, integrity, and reliability of the OT systems and associated applications. Due to the critical real-time operational requirements of OT systems, some flexibility in addressing the security controls in the standards is sometimes necessary to support their operation.

The IT Security Policy Web site also provides additional information on directives and standards, accreditation, and training: Risk Management Services Division.

[Contracted maintenance services and procedures for OT systems must be thoroughly documented.] The use of these services is particularly sensitive for OT systems, typically due to the isolation of the systems and considering the importance the system has when determining to use these services. Reclamation relies on OT assets and systems that generate power, treat and deliver water, and monitor and protect facilities, to fulfill our mission, and cybersecurity threats against these types of systems are increasing. Failing to protect these systems from cyberattack could harm Reclamation infrastructure, disrupt services, threaten community safety, and prevent us from fulfilling our mission. To prevent a successful attack on these systems, Reclamation must ensure they are isolated from external networks. Remote access to Reclamation OT is not allowed according to Reclamation policy IRM TRMR-130.

4.0 Management

Effective OT systems operations and maintenance programs depend on key management practices that include roles and responsibilities, planning, and monitoring. This "Management" section covers the general requirements for SCADA and EACSS OT systems. It is important to note that the scope of the requirements varies with size and criticality of the OT system.

4.1 Planning

Planning is required to manage OT systems effectively in the operations and maintenance phase of their lifecycle. Federal Information Technology Acquisition Reform Act requirements for planning and review provide business/maintenance planning for OT systems and provide future scope of costs for OT systems. FISMA requires each Federal agency to plan for security by developing, documenting, and implementing a risk-based IMT security program; assign security responsibilities to the appropriate officials; review IMT security controls; and strengthen the use of continuous monitoring. Reclamation's ACIO implements FISMA requirements through program capabilities.

5.0 Roles and Responsibilities

Responsibilities for OT systems operations and maintenance are to be formally assigned and documented. Suggested key roles and responsibilities are listed here:

5.1 Commissioner

Reclamation's Commissioner formally authorizes the operation of OT systems, based on their meeting minimum IT security requirements as established in Federal law.

5.2 Information Resource Officer

Reclamation's Information Resources Officer is responsible for certifying the security of OT systems and recommending investments for information technology used in OT systems.

5.3 Executive Owners

OT systems executive owners (e.g., regional directors) ensure systems support Reclamation's mission and are operated and maintained in compliance with relevant regulations.

5.4 Business Owners

OT systems business owners (e.g., area managers, power managers, operations managers, etc.) are responsible for providing guidance on mission requirements, support, and resources (funding and staff) for OT systems operations and maintenance activities.

5.5 Project/Program Manager

OT systems project managers plan and implement operations and maintenance programs for OT systems to support mission goals and objectives, monitor performance, and provide training for system users and support staff.

5.6 Support Personnel

OT systems support personnel (system managers, OT systems engineers, OT systems programmers, maintainers, technicians, etc.) are responsible for performing system replacements, software and equipment maintenance, system administration, communications support, and system health monitoring.

5.7 Security Manager

OT systems security managers are responsible for identifying, configuring, and managing security safeguards that include day-to-day reviews to ensure security controls are working and technical advice on security documentation, policy, and issues.

5.8 System User

OT systems users (e.g., operators, controllers, dispatchers, engineers, etc.) are responsible for following OT systems operating procedures and criteria contained in SOPs and for notifying system support staff when OT systems problems are observed.

6.0 Training

OT system operations, maintenance and support staff should have the knowledge necessary to maintain performance, reliability, and security of the OT system. This document only discusses the various types of training that should be provided. The training requirements for each staff member should be reviewed annually.

6.1 General Security Awareness Training

Security training (Cyber/Physical) also must be provided as required in the OT system security plan. Both operations and maintenance staff will be required to perform security training on a periodic basis to maintain expertise as it relates to their areas of responsibility. In addition, training related to personnel security, public trust responsibilities, and background investigations may be necessary. For more details, consult the OT system SSPP.

6.2 Operations Training

[OT system operators must be knowledgeable concerning the OT system-related responsibilities given to them.] This training includes the normal OT system operations, system monitoring and health checks, and troubleshooting and repair tasks. All new operators should receive initial training on all the topics. Training for existing staff should be reviewed yearly and refresher training performed as dictated by that review. Daily use of the OT system by operators may be considered training, but any changes to the operator interface requirements will require training to make sure operators understand procedures associated with the changes. When on-the-job training is performed, it should be documented to ensure training requirements for all the operations staff are completed and performed under proper supervision. Training should be provided in the examples listed below but are not limited to.

6.2.1 Normal Operations

This training should cover areas such as control console operation, display layouts, input methods, control systems, alarms, events, authentication procedures, and tagging. This training should cover all the areas required to perform OT system operations under normal OT system conditions. Training also should provide an understanding of alarms, events, and procedures for response. **[OT system operators must be knowledgeable concerning the impact of OT system operation on the facility(s) and its equipment, including required actions prior to overriding OT system control.] [OT system operators must be knowledgeable concerning the use of any informational Hazardous Energy Control Procedure tagging provided by the OT system.]**

6.2.2 System Monitoring and Health Checks

This training will cover issues associated with determining the condition of various elements of the OT system hardware, software, and communications. Training for OT system operators should include local procedures for reporting inaccurate data to system support staff. **[OT system operations staff must be knowledgeable concerning the use of any system monitoring tools they are expected to apply.]**

6.2.3 Troubleshooting and Repairs

Training should be provided to OT system operators in the areas where they are asked to perform troubleshooting tasks. Remedial tasks associated with OT system failure response performed by OT system operators also should be reviewed. Coordination procedures with OT system support staff during testing, repairs, and system upgrades should be discussed. **[OT system operators must be knowledgeable concerning those OT system corrective procedures they are expected to perform.]**

6.3 Support Staff Programming and Software Engineering Training

The primary maintenance functions for the OT system are performed by programmers, maintenance personnel, and software engineers tasked with performing maintenance, repairs and upgrades. OT system support staff should have knowledge of each element or module of the system**.** Training should be provided for maintaining the integrated system as well. **[OT system support staff must receive training as defined by the OT system Manager and/or the OT System Security and Privacy Plan (SSPP)]**. Training requirements should be reviewed on a yearly basis, and new training or refresher training performed as required. OT system support staff should be knowledgeable concerning any upgrades that are made to the system. Training includes the topics listed below.

6.3.1 General System

This training describes procedures to perform system start up, shut down, and system level troubleshooting.

6.3.2 Hardware

Training covers the various hardware elements of the system. The hardware elements might include consoles, display panels, computer equipment, communications equipment, and RTUs. Training covers hardware maintenance, configuration, and troubleshooting procedures.

6.3.3 Application and Control Software

This training focuses on the OT system application software. All applications such as generation control, voltage control, unit controls, and EACSS equipment controls should be covered during this training.

6.3.4 Software Development Tools

Training provides information on how to use development tools required for maintaining, repairing, and upgrading the application software.

6.4 System Administrator Training

The training provided to the OT system administrator focuses on the basic portions of the system. System administrators should have training on all hardware, operating systems, and driver configurations. For systems based on network backbones, basic network training, such as addressing, routing, protocols, masks, MAC addresses, access control lists, elementary firewalls, network security, etc., should be included in the administrators training. The system administrator training does not need to focus as heavily on the internal functionality of the OT system application software, but it should focus more on the system requirements for the software. New staff always should receive the full set of training as defined by the OT system

7.0 Program Review

O&M standards, FIST procedures, practices, and schedules that are in **[bold and bracketed]** are considered minimum requirements. Meeting these requirements is to be verified at power facilities during onsite reviews performed under the Power Review of O&M (PRO&M) process as defined by Directive and Standard FAC 04-01. Reviews of OT systems present additional challenges for the PRO&M process. Sensitive information is to be protected during the review process. OT systems can involve multiple powerplants with a centralized control center that may or may not be located at a Reclamation powerplant.

7.1 Monitoring and Reviews

Managing an OT system O&M phase requires monitoring costs, schedule, safeguards, and how well the system meets stakeholder and mission needs. Monitoring of planned maintenance versus actual improvements is performed periodically and on an annual cycle when business cases and maintenance plans are developed for OT system operations and maintenance are to be formally assigned and documented.

1. Major OT systems are required to monitor and report system cost, schedule performance, and conduct an operational analysis periodically as required by policy. The operational analysis is a standard methodology to assess and quantify the system's value in supporting mission goals and objectives (e.g., see OMB Circular A-11, Exhibit 300).
2. An Internal Control Review is required per Reclamation policy for OT systems. Identified deficiencies must be evaluated, and a corrective action plan must be developed and reported on in the system's Plan of Action and Milestones (POA&M).
3. OT system contingency plans, incident response plans and supplement, and recovery plans must be exercised as required by Reclamation policy. Reports of exercises are required.
4. Recommendations identified during onsite reviews conducted under the PRO&M program for OT systems operations and maintenance are to be evaluated, actionable improvements must be planned, and status must be reported at annual regional Reclamation Power O&M meetings until completed.

8.0 Operational Technology Fundamentals

The most important goal for any OT system is to provide operations staff with a tool that allows them to monitor and control their plant and facility equipment under normal conditions efficiently and reliably. This section provides general requirements for normal operations tasks when the OT system is functioning properly, and no problems or failures exist. It focuses on the consoles, displays, plant equipment monitoring, controls, and other normal operations requirements.

A particular OT system's performance normally is defined in the original design specifications. However, differences from those specifications do occur, and those differences can be found in design updates or "as built" drawings. The current documentation for the system is the most reliable source for ICS performance. Please refer to those documents when addressing any system performance issues.

8.1 Workstations and Displays

The primary interface between the operator and the OT system is via workstations and various types of displays. The workstations allow the operator to input commands and data to the OT system as well as to provide the operator with the status of the powerplant and facility equipment. Displaying data is the most critical element of the workstations. Critical functions include:

- Display of real-time data

- Command interface (equipment and process control)
- Data input capabilities
- Screen navigation tools

As the workstations and displays are key technical components for "supervisory control," normal performance characteristics should be reviewed. Characteristics that should be reviewed include reliability, ease of use, visibility or clarity, effectiveness, and training on modifications or revisions to workstations and displays. Large displays such as mimic boards or panel displays may be used for system overviews, video monitoring for security, and access to local news and weather conditions. HMI such as displays, workstations, and input devices function as operators need; they are maintained, losses of visibility of displays are to be corrected in a timely manner, and critical HMI should have spares on hand.
It is recommended that redundancy be provided where possible, so that a single display failure can be tolerated and still leave the operator able to view system data and perform controls. Multiple workstations and/or multiple view terminals should be provided as necessary to maintain operator functions through display equipment failures.

System overviews and menus should be provided to allow navigation easily through the input options. Input devices such as workstation cursor controls (trackball, mouse, keyboard, etc.) must be provided to perform screen control and input selection.

8.2 Equipment and Facility Monitoring

Monitoring equipment and facility status is a critical element of all OT systems. If inaccurate status information is given, equipment misoperation could result, disrupting key processes such as power generation and water releases. Data reliability and refresh rates from OT system equipment should be maintained at an adequate level. Reliability of the OT systems that support operations and protection at National Critical Infrastructure sites should be maintained above 99.5 percent on average for normal operations. This is approximately 44 hours of down time in 1 year. Reliability of the OT system may be defined in a variety of ways, depending on the system architecture. However, reliability goals should relate to the ability to provide critical operations support. **[Reliability goals should be set for all OT systems.]** This may depend on the critical nature of the controls, or the original system specification goal may be used. Information about reliability should be calculated and recorded so that corrections can be made if the reliability reaches unacceptable levels.

Refresh rates for the data also are important. **[For OT systems that support powerplant operations, the data display must reflect any change in status within a reasonable period as required by the system design specifications.]** OT systems within Reclamation should focus on meeting data updates to the operator to occur within a maximum of 4 seconds.

The quality of status data always should be provided. Data quality monitoring should include failure conditions (not being updated), alarm conditions, and out-of-range conditions as a minimum. Data failures should be tracked, and time tagged.

8.3 SCADA Control Modes and Unit Controls

[The capability to override OT system controls must be provided at the unit controls for a particular generator or at the local controls for any type of equipment.] This feature is provided by a control switch such as the unit control, mode selector switch, or the "43" selector switch. The 43 has three switch positions or modes: Manual, Local Automatic, and Supervisory. In addition, where a system is digital, a physical 43 switch is required to allow the generator and its control to be separated from the plant OT system. **[Where a system is fully digital, a physical means of switching the machine to local automatic shall be provided to prohibit the plant or OT system from causing the machine control to operate.]**

8.3.1 Local Manual

This mode disables all OT system controls. The generator output is adjusted manually by an operator, either locally or remotely, without automatic feedback from system conditions. In this mode, only manual controls can be performed from the control board or near the local equipment.

8.3.2 Local Automatic

This mode provides for automatic controls locally for the generator or other plant equipment. The generator operates under automatic control based on local signals, such as frequency or tie-line bias, but not directly controlled by the Balancing Authority (BA). For example, the OT system may be used to start a generator or a pump. For some sites, the generator or other equipment also may be controlled using equipment external to the OT system such as relays designed to perform start or stop functions. A local display or panel may be used to allow the operator to initiate the local control functions. No remote control of the generator from a control center or any other remote-control room is allowed in this mode.

8.3.3 Supervisory

This mode allows the generator or other equipment to be controlled remotely by an operator located at a control room or initiated by control logic within the system application software. All the OT system controls provided can be performed by the remote operator. Local Manual or Local Automatic OT system controls are no longer possible in this mode (apart from emergency shutdown (86) or headgate close control).

The SOP or operations orders for the facility should describe how to use these modes. In addition, the SOPs should note if notifications are required before or after changing the status of the control switch.

8.4 Controls and Applications

[The OT system must provide the operator with the control capabilities necessary to operate the facility.] The control capabilities may include manual operation where applicable. Direct control of equipment such as pumps, breakers, valves, and gates should be provided in a way that allows the operator to perform control tasks reliably, efficiently, and safely. The operator should not use OT system control when the equipment status is questionable. Automatic controls always should be disabled (and tagged if capable) when inputs are questionable and cannot be observed by a reliable source per OCMP requirements.

Software applications support controlling equipment such as startup, shutdown, and set point controls (generation, voltage, and flow). Software applications also may support power system control, power system reliability, water system scheduling, and power system scheduling as required. Each system should identify what controls it considers critical. Such controls could include operation of gates and valves to maintain water delivery, gate control setpoints, generator set points, distribution of automatic generation control, etc. In addition, the frequency of testing of those critical controls should be established. **[Critical controls will be tested on their defined FIST 4-1B frequency].** The controls should be configured to provide the operator with final responsibility for the reliability and safety of the controlled facilities. For Reclamation OT systems that provide powerplant set point controls (generation and automatic voltage), critical features including minimum response requirements should be tested when changes in plant configuration take place.

[Powerplant set point controls must allow governors to respond properly during a frequency disturbance on the power system. Automatic voltage control, as well as facility level voltage control systems or loops, must allow for proper voltage regulator response during power system disturbances.] These controls should not negate the unit's response to system voltage and frequency deviations during a disturbance, unless it is to keep the unit within its safe operating range.

8.5 Alarms and Event Recording

An alarm system should be provided to display alarm conditions that occur within the plant. The alarm system should allow setting, acknowledging, and clearing alarms. **[OT system operators must be trained, and have SOPs available, to respond to an alarm and what actions are to be taken.]** In some cases, methods to disable alarms will be provided to override nuisance alarms. **[The cause that requires an alarm to be disabled must be addressed on a timely basis.]** The OT system should provide the ability to track overridden alarms.

Every effort should be made to address alarms as they occur as well as to avoid setting alarms that do not require operator attention. OT system staff should work closely with maintenance personnel to minimize the number of alarms presented to the operator. A separate maintenance/test network may be a good option to allow adequate information for engineering purposes while preserving the security and operability of the OT system.

The OT system will record significant equipment alarms, events, and OT system changes in a log. The OT system should use time tags for both alarms and events and use a satellite or Global Positioning System clock for time tag accuracy. Error logging and time tagging should use the Universal Time Code (UTC) where practical. In addition, universal time should be used for the system such that any system covering multiple time zones should use one standard, uniform time across the entire system.

Sequence of Event (SOE) recording should be possible with the OT systems. The SOE recordings may be an aid to unexpected events investigators in determining what caused an event. See FIST 6-3, Unexpected Event Reporting. The Regional Power Office or Power Resources Office should be consulted to determine the requirements, if any, for SOE for any power-related unit, plant, or OT system. For example under NERC PRC-002-4, the Sequence of Events (SOE) or Sequence of Events Recording (SER) data must be retained regardless of whether an event has occurred for applicable BES Elements.

8.6 Shift Change

The OT system must fully support operator shift change requirements. It should provide reliable log-in/log-out procedures and, where possible, automatically clear previous shift preferences while applying settings for the incoming shift.

No data, alarms, or special conditions should be lost or disrupted during the transition. Critical information from the outgoing shift that is needed by the incoming team must be preserved and accessible. The handover process should ensure that all information exchanged between operators is accurate, clear, and complete.

8.7 Daylight Saving Time

The OT system must support automatic transitions to and from daylight saving time where applicable. Time changes should occur precisely at the designated moment, with all system functions continuing to operate correctly under the new time setting.

There should be no data loss or duplication during the transition. All scheduling and time-tagging features must adjust accurately to reflect the time change. If manual intervention is required, clear and documented procedures must be in place.

8.8 Special Operating Procedures

The SCADA system should provide a visual tag to alert an operator to the status of facility equipment. Any condition that requires physical tagging of equipment should be supported, including clearances, hot line orders, and special conditions. **[The visual tags must provide a visual indication of the condition for the operator, are in addition to the actual equipment tags, and are not used to provide the actual lockout features.]** It is important that the tagging features are used properly, so that the current condition is indicated to the operator. See FIST 1-1 for additional information regarding the Hazardous Energy Control Program and OT system tagging.

For OT systems lockout and tagout conditions for equipment always should be coordinated so that no automatic operations can occur during these conditions. Isolating the equipment using the "43" control switch should be incorporated into the switching orders. Switching to manual or local automatic may allow data to be transmitted from the unit or equipment to the OT system but should preclude any data being transmitted to the unit from the OT system. If status of equipment can be monitored safely during outage conditions, the OT system should provide the operator with that status.

8.9 System Wiring

OT system wiring/cabling should be maintained in good condition. **[All OT system wiring and cables, including network cables, shall be legibly labeled.]** All wires and cables must be terminated according to manufacturer/design recommendations and labeled at termination points. Cables should be confined to trays, conduit, and raised floor areas. Where practical, electric power provided to plant conditioning inputs (status inputs to the SCADA) should be uninterruptable to improve the likelihood that critical status information will be available under various failure scenarios.

8.10 Equipment Power

Three options are normally available when selecting power to be used for OT system equipment.

1. An Uninterruptible Power Supply (UPS) (station class) is used to power computers and equipment at a control center and at plant locations. A UPS normally is powered from a station alternating current (ac) power source.

   In many cases, the UPS may support only a percentage of OT system functionality during a power failure. It is important that this functionality be defined, and that operations and support staff understand what will function when the OT system is operating only on the UPS. When possible, testing should be performed to verify the OT system functions as

designed. The UPS must be capable of maintaining the OT system operational for a preset minimum period (based on system design) following a failure of station power. The minimum period for OT system operation by the battery system will vary from site to site but should be set based on the time needed to complete facility emergency power procedures or to prepare for manual operations without the OT system functions. Tests of an input power failure for the OT system should be performed once the system is operational, and tests should be repeated when a change in UPS configuration or potential battery draw occurs or as specified by the manufacturer.

2. Station direct current (dc) power with an inverter is used to develop the ac power required for OT system or other critical equipment. This approach may be used for RTUs or remote equipment where access to the station battery makes this solution an option. When this option is used, maintenance and testing should be performed according to manufacturer specifications for the UPS, FIST 3-6, and FIST 4-1B instruction.
3. The equipment is powered directly by station ac power. This option may be selected for noncritical OT system equipment that will not have to operate during a station service failure.

9.0 Maintenance Program

There are issues that should be considered when maintaining Reclamation OT systems. Every effort should be made to avoid failures by performing: 1) general maintenance, 2) proper system monitoring and health checks, and 3) manufacturer recommended maintenance. When failures occur, sound methods of troubleshooting and performing repairs should be used. Contingency plans and backup/recovery procedures should be in place to recover from failures quickly.

Consider both the timing and method of performing maintenance, as well as its potential impact on the operational system. If maintenance requires taking key system capabilities temporarily offline, it should be scheduled during periods of minimal operational impact. Additionally, ensure that qualified staff are available to manually operate the controlled facilities if needed during the outage.

9.1 General

This FIST provides guidance and instruction to perform preventative maintenance and functional test procedures on alarm panels, enclosures, balanced magnetic switches (BMS), magnetic locks, electronic strikes, motion detectors, cameras, digital/network video recorders (DVR/NVR), network components, computers, power supplies and uninterruptible power supplies (UPS), vehicle barriers, and other miscellaneous OT system devices.

Maintenance recommendations provided in this FIST may be used to satisfy the NIST 800-53 requirements. The recommendations provided are specific to Reclamation OT systems.

Reclamation Manual Directives and Standards SLE 03-02, Facility Security, requires that all EACSS equipment will be maintained in good working order to maximize security effectiveness and longevity.

9.1.1 Documentation

Complete and accurate documentation is essential to an effective maintenance program. Routine preventive maintenance usually involves some form of evaluation of equipment to determine if some additional maintenance is needed to ensure the equipment can perform reliably until next evaluation. The results of the evaluation and any additional maintenance identified because of the routine preventive maintenance are included in the documentation of the equipment condition. **[Whether performing preventive, predictive, condition-based, or reliability centered maintenance, documenting equipment condition and the maintenance task is required]**.

[A maintenance log for OT systems must be maintained.] The type of maintenance log (e.g., physical or electronic) and where it is kept (e.g., at each site or at a central location) is to be determined by the system manager. The maintenance log should outline all maintenance activities performed on the system. The record should include, as a minimum, the date of the activity, the party responsible, a brief description of the activity performed, and a list of system component(s) affected. Maintenance logs may be combined with a version control function required to coordinate system upgrades as desired. Examples of maintenance logs include, but are not limited to, CARMA work orders, Excel spreadsheets, and physical logbooks.

9.1.2 Repair/Replacement Parts

Spares should be acquired and maintained in proper working order in anticipation of a failure. **[Spare hardware for all critical single point failure items must be maintained. At least a single spare or provisions of equipment replacement must be maintained for all critical equipment.]** Spares may not be needed for redundant systems. For hardware that occurs in large numbers within an OT system, a minimum of 10 percent of the hardware should be maintained

as spares. Spare equipment should be fully configured, operational, and tested when possible. If configuration is required prior to operation, then configuration procedures must be clearly documented. Documentation should be current and should apply to the existing configuration. Spares should be stored in a manner to minimize exposure to fire or other hazards. **[A spare parts inventory for all critical single point failure items must be maintained for the OT system.]** The inventory should identify a list of spare parts and storage location. Review of the spare parts inventory should be conducted periodically with signature and date of review.

9.1.3 Miscellaneous Maintenance Requirements

9.1.3.1 *Electrostatic Discharge Sensitive Devices*

CAUTION

Observe precautions for handling electrostatic discharge (ESD) sensitive devices. Ensure personnel are grounded using an ESD wrist strap or other personal grounding devices to prevent damage to electronic components. Be aware of heat and moving components. Follow all applicable ESD prevention procedures. Utilize appropriate Personal Protective Equipment (PPE) as required.

9.1.3.2 *Environmental Controls and Fire Protection*

Environmental controls for OT systems should be monitored, checked for proper operation, and maintained per requirements set by the manufacturer. Operating an OT system at high temperatures can degrade the computer equipment, cause a safety shut down, or equipment failure. Cooling systems should be maintained in good condition, and OT system equipment should be maintained at environmental conditions that meet the recommended limits set by the manufacturer.

Fire protection systems/equipment should be provided for OT system equipment and maintained per manufacturer requirements. The operability of any fire protection system should be verified according to FIST 4-1B maintenance schedule. The proper class of fire retardants should be employed to ensure that fires can be extinguished while minimizing shock hazards and OT system equipment damage. Refer to the National Fire Protection Association (NPFA) in the standards and reference list.

Storage areas should provide appropriate environments and fire protection for the documents and spare equipment they contain. The OT system and storage areas should be kept clean and orderly and free of unnecessary hazards.

9.2 System Monitoring and Health Checks

When maintaining a reliable OT system, developing and using the proper system monitoring tools are important. Health monitoring of all software and hardware elements is recommended. A full system monitor that allows OT system maintenance staff and operations staff to determine the status of modules or elements of the system also is recommended. Staff should understand the alarms associated with health checks and failure detections. A log of these failures should be maintained. Health monitors should be tested when placed in service or if system hardware or software configuration changes to the OT system warrant repeating the testing.

Monitoring of functionality should be provided for the OT system elements discussed in these subsections.

9.2.1 Hardware Functionality

The proper function of individual hardware elements of the OT system should be monitored continuously. For example, individual computer nodes in the system should have a status monitor to indicate when the node is functioning properly. Input and output equipment also should be monitored for proper function or have status monitors to detect problems.

9.2.2 Application Functionality

Software applications also should indicate when they are functioning properly. Control applications, such as automatic generation control, can fail without a corresponding hardware failure. It should be possible to detect these application failures by viewing or monitoring a status indication.

9.2.3 Communication Functionality

Communication systems are an important part of all OT systems, and the proper performance of these systems is critical. Communication systems may include microwave, radio, telephone, cellular telephone, satellite, and fiber optic systems. These systems also include equipment such as modems, radios, multiplexers, switches, and routers. Generally, both online monitoring and test procedures are used to verify proper operation of communication systems. Periodic reviews and tests should be employed to detect any changes in equipment performance. Those changes should be investigated to determine equipment degradation that could lead to ultimate failure.

9.3 Maintenance

Preventive maintenance on various elements of the OT system equipment is required to maintain equipment performance. These systems operate continuously and, in many ways, are self-

diagnosing; but some maintenance and testing of these devices are necessary to ensure system integrity and identify potential failures. Individual recommendations should not be used blindly without thorough consideration and testing to gauge their impact on an in-production system. Preventative maintenance should be completed as scheduled while considering the effects to the online system.

Maintenance technicians/mechanics should work with IT system administrators, facility operators and security personnel to coordinate OT system maintenance. Completion documentation (completed workflow/CARMA work orders) of these activities may be used as evidence of compliance with other requirements (e.g. Federal Information Security Management Act, North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP), etc.).

NOTE

Alarm monitors (i.e., security guards or control center operators) must be notified before any preventative maintenance inspection or functional test is performed. Activities such as removal of power/communications, opening cabinets, or adjusting/removing sensors will generate alarms. Devices removed from or out of service will be documented during the PM or Functional Test procedure as such. While performing the preventative maintenance and functional tests, resolve any newly discovered or previously documented maintenance issues if possible. If a repair item is identified during the preventative maintenance and can be repaired on the spot, document the repair under the preventative maintenance work order. If the repair requires further action, open a new work order, and report the malfunction to appropriate personnel (e.g., Area Office Security Coordinator).

9.3.1 OT System Hardware

The manufacturer of individual OT system components normally provides recommendations for hardware components that require either periodic maintenance or periodic testing. Internal equipment such as fans, batteries, or cabinet filters all may require periodic checks and/or maintenance. In some cases, such as input/output hardware, hardware may need to be tested. This maintenance should be performed based on manufacturer recommendations wherever possible. Depending on the environment of the installed hardware maintenance intervals and instructions may need to be adjusted to account for the environmental factors of the installed location.

9.3.1.1 *Enclosures*

[Enclosure Maintenance]

1. Inspect enclosure.
    a. Inspect exterior of the enclosure for damage.
    i. Minor scratches and dents are to be expected. Enclosures located in temperature-controlled areas which have minor paint damage are acceptable.

   ii. Fiberglass/composite enclosure: check for cracking, damage, and degradation (UV damage, abrasion, fiber blooming, etc.).
   iii. Major paint damage (larger than 1") or paint damage on devices in uncontrolled climate areas must be repaired.
   b. Inspect utilized knockout holes to ensure conduit/enclosure connecters are tight and cables are not being damaged during transition.
   c. Inspect knockout holes not being utilized to ensure they have original plugs or are plugged using appropriate equipment/ knock out blanks.
2. Repair or replace as necessary.
3. Clean the exterior and interior.
   a. Use a dry cloth, compressed air, or an electro-static discharge (ESD) safe vacuum cleaner with a soft brush attachment on the end of hose to remove dust, dirt, or debris in interior of enclosure. Do not use damp cloth on the interior of the enclosure, near electrical components, or near security panels/devices inside the enclosure.
   b. A damp cloth can be used to clean the *exterior* of enclosure.

9.3.1.2 *Alarms Panels*

[Alarm Panel Maintenance]

1. Inspect alarm panel.
    a. Inspect the alarm panel for damage (electrical or physical), loose connections, or foreign debris such as dirt, dust, and metal shavings.
    b. Inspect the alarm panel to ensure the LEDs are properly illuminated to show operational status (refer to system owner's manual for information on LED status).
    c. Inspect the on-board battery status. If it is greater than three years old, showing symptoms of failure, or is generating an alarm, replace it. See manufacturer's recommendation.
2. Repair or replace as necessary.
3. Clean with compressed air to remove dust, dirt, or debris.

9.3.1.3 *Card Readers*

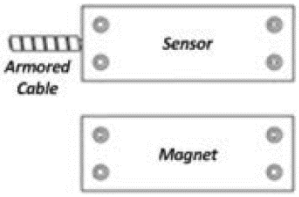
[Card Reader Maintenance]

1. Inspect card reader.
    a. Inspect the card reader for damage (electrical or physical) and loose connections.
    b. Inspect the card reader to ensure it is securely mounted.
    c. Inspect LED lights and light bars to verify proper operation.
2. Repair or replace as necessary.
3. Clean exterior of card reader with dry or damp cloth as needed to remove oil, dust, and debris.

9.3.1.4 *Balanced Magnetic Switches*

[Balanced Magnetic Switch (BMS) Maintenance]

1. Inspect BMS.
    a. There should be no metal filings or other debris on the sensor.
    b. Wire insulation should be free of damage and in good condition (free of nicks, exposed copper, etc.).
    c. Armored cable should be free of nicks, gaps, and burrs which could damage the wiring, device, or personnel.
2. Repair or replace as necessary.
3. Clean with dry or damp cloth as needed to remove oil, dust, and debris.

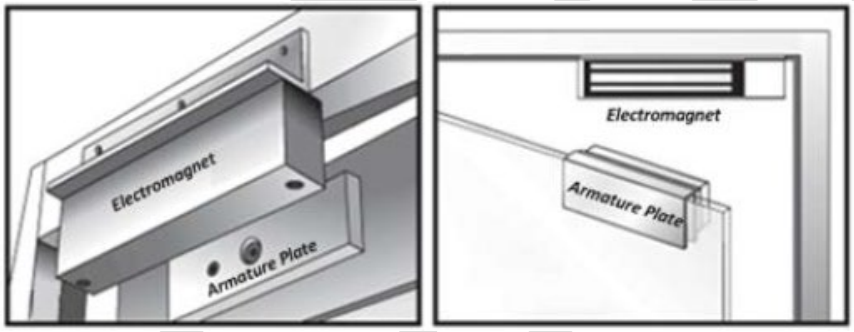


Depicts one example of a BMS

9.3.1.5 *Magnetic Locks*

[Magnetic Lock Maintenance]

1. Inspect magnetic lock.
    a. Verify proper alignment of metal plate attached to door and electro-magnetic assembly on frame. See manufacturer's documentation for proper alignment procedure.
    b. There should be no metal filings, rust or other debris on metal parts.
    c. Door and frame should be structurally sound and able to support the magnetic lock.
2. Repair or replace as necessary.
3. Clean with dry or damp cloth as needed to remove oil, dust, and debris.

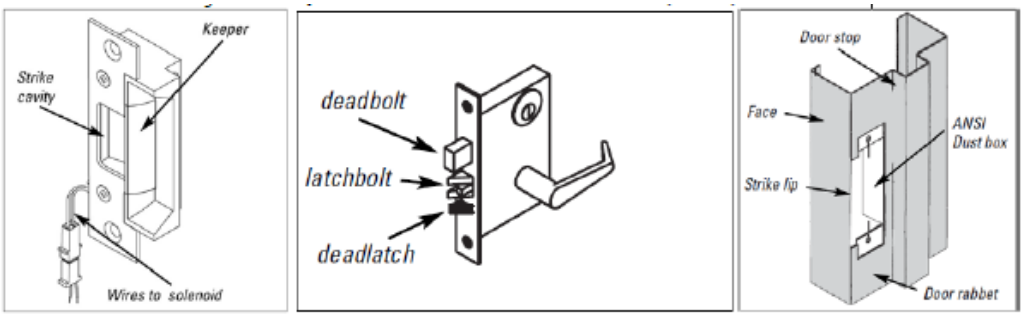


Depicts one example of magnetic lock door hardware.

9.3.1.6 *Electronic Strikes*

[Electronic Strike Maintenance]

1. Inspect electronic lock/strike for missing hardware.
2. Inspect visible wire. Should be free of damage and in good condition (free of nicks, exposed copper, etc.).
3. Armored cable should be free of nicks, gaps, and burrs which could damage the wiring, device, or personnel.
4. Repair or replace as necessary.
5. Clean with dry or damp cloth as needed to remove oil, dust, and debris.



Depicts examples of electronic strike components.

9.3.1.7 *Motion Detectors*

[Motion Detector Maintenance]

1. Inspect motion detector.
    a. Inspect for missing hardware.
    b. Inspect for damage (e.g., cracked housing, proper mounting, etc.)
2. Repair or replace as necessary. If motion detector is damaged, order new motion detector and replace as soon as possible.
3. Clean with dry or damp cloth as needed to remove oil, dust, and debris.

9.3.1.8 *Tamper Switches*

[Tamper Switch Maintenance]

1. Inspect tamper switch.
    a. Inspect plunger for mechanical actuation (plunger moves freely in and out).
    b. Inspect for loose wiring and exposed copper.
2. Repair or replace as necessary.
3. Clean with dry or damp cloth as needed to remove oil, dust, and debris.

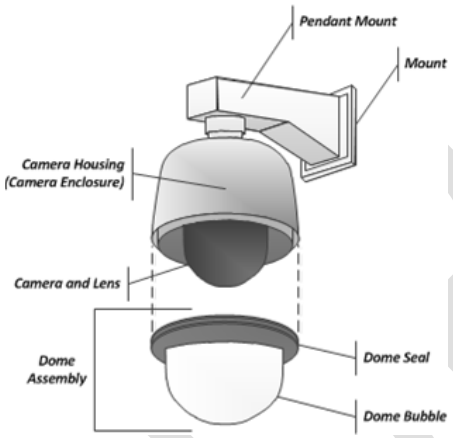
9.3.1.9 *Cameras*

[Fixed, PTZ and Thermal Camera Enclosure Maintenance]

Refer to enclosure instructions above.

Dome Camera (Fixed, PTZ, and Thermal)

1. Inspect dome camera.
    a. Inspect cables, connectors, and cable shielding between enclosure, pole and camera for abrasions, cracks, or deterioration.
    b. Inspect for damage on the camera housing, including insect damage, lightning damage, and/or other mechanical failure.
2. Repair or replace as necessary.
3. Clean camera housing, dome bubble, and lenses.
    a. Use a cloth to wipe down the exterior of the camera housing; if needed use a mild detergent water solution and wipe off using a cloth.
    b. Remove the dome assembly to access the inside of the dome; use a micro-fiber cloth to remove dirt or dust buildup inside the housing.
    c. The dome bubble over the camera and lens can be cleaned using a lens-cleaning solution and micro-fiber cloth or tissue paper approved for camera lenses (glass). Never use paper towels; paper towels may scratch the dome bubble.
    d. When complete, replace the dome-bubble to original position, ensuring the dome is adequately sealed.



Depicts one example of a dome camera.

Box Camera (Fixed, PTZ, and Thermal)

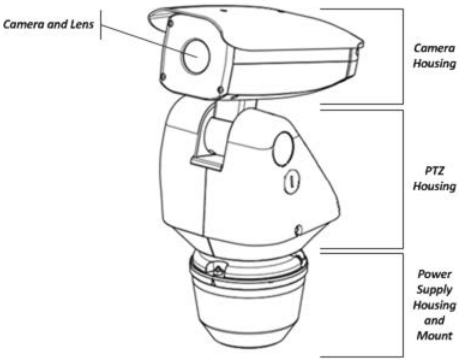
1. Inspect box camera.
    a. Inspect cables, connectors, and cable shielding between enclosure, pole and camera for abrasions, cracks, or deterioration.
    b. Inspect for damage on the camera housing, including insect damage, lightning damage, and or other mechanical failure.
2. Repair or replace as necessary.
3. Clean camera housing, housing window, and lenses.
    a. The lens of the camera is easy to damage. Clean only if needed.

b. Use a cloth to wipe down the exterior of the camera housing; if needed use a mild detergent water solution and wipe off using a cloth.
c. Open the camera housing, if dirty use a micro-fiber cloth or compressed air to remove dirt or dust buildup inside the housing.
d. The window in front of the camera housing and lens can be cleaned using a lens-cleaning solution and micro-fiber cloth or tissue paper approved for camera lenses. Never use paper towels; paper towels may scratch the window.
e. When complete, close the camera housing.

Depicts one example of a Box/Fixed camera.

Sealed Camera (Fixed, PTZ, and Thermal)

1. Inspect
    a. Inspect cables, connectors, and cable shielding between enclosure, pole and camera for abrasions, cracks, or deterioration.
    b. Inspect for damage on the camera housing, including insect damage, lightning damage, and or other mechanical failure.
2. Repair or replace as necessary.
3. Clean camera assembly (camera housing, PTZ housing, and power supply housing and mount) and lenses.
    a. Use a dry cloth to wipe down the exterior of the camera housing; if needed use a mild detergent water solution and wipe off.
    b. The lens of the camera can be cleaned using a lens-cleaning solution and micro-fiber cloth or tissue paper approved for camera lenses. Never use paper towels; paper towels may scratch the window.



Depicts one example of a sealed camera.

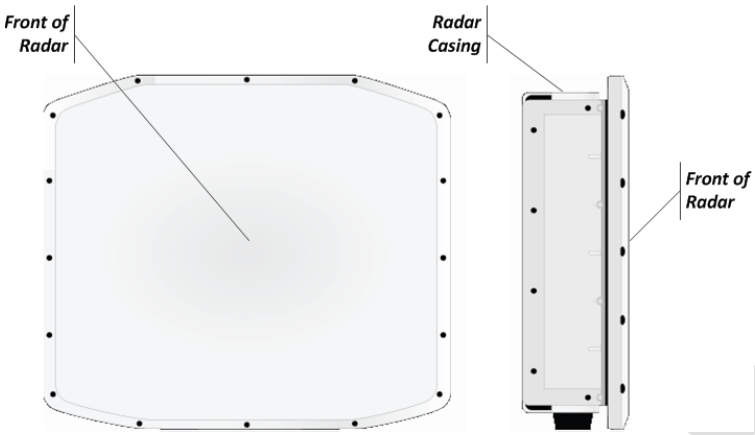
[Camera Pole Maintenance]

1. Inspect pole.
    a. Wood pole: check for cracking, damage, and rot.
    b. Metal pole: check for cracking, damage, metal fatigue, mechanical damage, and corrosion.
    c. Concrete pole: check for cracking, damage, and exposed rebar.
    d. Fiberglass/composite pole: check for cracking, damage, and degradation (UV damage, abrasion, fiber blooming, etc.).
2. Repair or replace as necessary.
3. No cleaning required.

9.3.1.10 *Radar*

[Radar Maintenance]

1. Inspect radar. Radars are sealed units and only the exterior should be inspected. The front of the radar is made of a thin material which is transparent to RF transmission. This material is easy to damage. Take care when working on the radar.
    a. Inspect casing for damage. Paint damage on casing must be repaired.
    b. Inspect front of radar for rips or holes.
    c. Inspect wiring and raceway. Ensure connector is secure.
    d. Inspect mount and cable. Verify mounting hardware is tight and free of corrosion.
2. Repair or replace as necessary. Do not repair damage to the front of the radar. If damage is found, other than the paint damage to the casing noted in a. above, the unit must be replaced.
3. No cleaning required if inaccessible.



Depicts one example of a radar.

9.3.1.11 *Video Recorder*

[Digital/Network Video Recorder (DVR/NVR) Maintenance]

1. Inspect DVR/NVR.
    a. Inspect connectors for damage and exposed copper.
    b. Inspect wire connection points to ensure they are tight and not stressed (e.g., other equipment and or cabling is not weighting down wiring).
    c. Inspect wiring for damage.
    d. Inspect for tampering.
    e. Verify optical disk drive tray opens/closes properly.
2. Repair as or replace necessary.
3. Clean enclosure using a dry cloth to remove dust, dirt, and debris. If the DVR/NVR has a fan, clean fan assembly using compressed air.

9.3.1.12 *Network Components*

[Network Component Maintenance]

1. Inspect network device (e.g., switches, encoder, decoder, etc.).
    a. Inspect connectors for damage and exposed copper.
    b. Inspect wire connection points to ensure they are tight and not stressed (e.g., other equipment and or cabling is not weighting down wiring).
    c. Inspect wiring for damage.
    d. Inspect for tampering.
    e. Listen for any excessive vibrations or noise from the fan or power supply.
2. Repair or replace as necessary.
3. Clean enclosure using a dry cloth to remove dust, dirt, and debris. If the network component has a fan, clean fan assembly using compressed air.

9.3.1.13 *Computers*

[Computer Maintenance]

Procedure for External Computer PM

1. Inspect computers (e.g., workstations and servers) and peripherals.
    a. Inspect connectors for damage and exposed copper.
    b. Inspect wire connection points to ensure they are tight and not stressed (e.g., other equipment and or cabling is not weighting down wiring).
    c. Inspect wiring for damage.
    d. Inspect for tampering.
    e. Listen for any excessive vibrations or noise from the fan or power supply.
2. Repair or replace as necessary.
3. Clean enclosure using a dry cloth to remove dust, dirt, and debris. If the computer has a fan, clean fan assembly using compressed air.

Procedure for Internal Computer PM

CAUTION
Observe precautions for compressed air by powering down all electronic devices due to flammable propellant.

1. Power down the computer.
2. Inspect the interior of the computer.
    a. Inspect connectors for damage and exposed copper.
    b. Inspect wire connection points to ensure they are tight and not stressed (e.g., other equipment and or cabling is not weighting down wiring).
    c. Inspect wiring for damage.
    d. Listen for any excessive vibrations or noise from the power supply or system fans.
3. Repair or replace as necessary. Verify, using manufacturers recommendations, whether the part is a reparable or replaceable part. Some failures may require replacement of the computer.
4. Clean interior of computer and fans using compressed air to remove dust, dirt, and debris.

9.3.1.14 *Programable Logic Controllers*

Programable Logic Controller (PLC)

1. Power down the system.
2. Inspect the condition of the PLC.
    a. Check that all connections are secure by inspecting plugs, sockets, and terminals for loose connections. High-vibration areas should be checked more often, especially paying attention to fasteners like screws and bolts.

   b. Check for scorch marks and, loose wiring on components and at terminal connections.
   c. Examine the CPU and the other PLC modules visually for signs of wear, warping, distortion, or overheated parts, such as burnt scents or discoloration.
3. Repair or replace as necessary.
4. Clean power supply/board using compressed air to remove dust, dirt or debris. Remove all dirt or dust that has accumulated on the PLC components including its I/O modules, such as the CPU unit and the I/O system.

[Other Miscellaneous Devices]

Some devices are too varied and minor for specific instructions under this FIST. As with the other specific equipment preventative maintenance procedures noted in the FIST, these types of devices should be inspected, and cleaned as needed to ensure the continued operation (refer to manufacturer's instructions for specifications).

9.3.1.15 *Batteries and Power Supplies*

NOTE: FIST 3-6, Storage Batteries Maintenance and Principles, provides specific instruction on the testing, inspection, and replacement of batteries. However, the FIST requirements only apply when batteries are over a certain voltage and current level. Follow FIST manual where applicable. If the FIST threshold is not met, perform the following preventative maintenance procedure.

[Battery/Battery System and Power Supply/Board Maintenance]

[Battery/Battery System]

1. Power down the system.
2. Inspect battery.
   a. Check battery for warping, cracking, or bulging.
   b. Check battery terminals for corrosion.
3. Repair or replace as necessary. If battery shows warping, cracking, or bulging, battery must be replaced. It is recommended that the batteries be replaced every three years or according to manufacturer's replacement recommendations. Annotate within the work order and write date replaced on the battery.
4. Clean exterior using a dry cloth to remove dust, dirt, or debris.

[Power Supply/Board]

1. Power down the system.

2. Inspect power supply/board (e.g., Altronix PD8, Altronix power supplies, 24VAC power supplies, etc.)
    a. Check for cracking of components and wiring.
    b. Check for scorch marks and, loose wiring on components and at terminal connections.
3. Repair or replace as necessary.
4. Clean power supply/board using compressed air to remove dust, dirt or debris.

9.3.1.16 *Vehicle Barriers*

[Vehicle Barrier Maintenance]

1. Power down the system and lock-out tag-out the vehicle barrier.
2. Inspect automated vehicle barrier (AVB) equipment:
    a. Related safety devices (including induction safety loop detectors) and warning signs/signals/lights.
    b. Check and adjust barrier operating speeds (where appropriate).
    c. Covers and protective plates on equipment to prevent water or wildlife damage.
    d. Hoses for damage, cracking, leaking and wear.
    e. Safety signs, decals, and appropriate stickers and replace as necessary.
    f. Hinge pins, lubricate when needed.
    g. Relays, motor starters, and switches for signs of contact wear.
    h. Indicator lights and traffic lights for proper operation; replace bulbs as necessary.
    i. Areas that need touch-up paint or corrosion protection.
    j. All cabling and wiring for control and operating devices for wear, indications of pinch or drag during operation, etc. (Consider re-routing, additional protection (armoring), or replacement where wire or cable shows excessive wear or damage that could result in grounding-out or interrupting power or signals.)
3. Repair or replace as necessary.
4. Clean complete barrier system using appropriate methods, which may include high pressure water/air, manually brushing, or other means (alone or in combination).
    a. Foundation, hinges, and tracks to prevent interference from dirt, stones, or trash; pick up remaining bits with small handheld broom and dustpan.
    b. Remove debris from all sump areas and system cabinets; clean and flush drains.
5. For system specifics and hydraulic fluid capacities, refer to the manufacturers manual and recommendations.

9.4 Testing

The functional testing process verifies the correct operation of all components within the circuit path. Therefore, functional testing requires activation of an initiating device (in the field), monitoring of the point into the OT system for correct operation, and activation of the correct OT system output point as anticipated. If any issues are identified during the functional test that

cannot be resolved at the time of the functional test, it should be logged, and a corrective maintenance work order should be opened.

NOTE
When testing alarm points annually, it is necessary to include the alarm monitor and maintenance personnel as part of the assessment. The alarm monitor located at the alarm monitoring station will monitor and verify the status of the alarm point under test. Maintenance personnel will perform the functional test and document the outcome of the alarm point under test.

Upon completion of sensor testing, ensure the alarm monitor acknowledges and or deletes the alarm and restores the system to its normal state.

9.4.1 Access Control

[Alarm Panel Functional Test]

Ask alarm monitor to verify panel is on-line using the ESS software at the alarm monitor client workstation or from the display at the Intrusion Detection System (IDS) Panel. The alarm panel will be either off-line or on-line.

[Card Reader Functional Test]

For a card reader that is not routinely used, the documented functional test of the electronic strike or magnetic lock can also be used to satisfy the functional test of the card reader.

9.4.2 Sensors

[BMS Functional Test]

1. Use a key to open the door. The alarm monitor should receive a door forced open alarm.
2. Close the door. Select and acknowledge the door forced open alarm. The alarm should clear.
3. Using a valid card, gain access to the door by presenting it to the card reader. Alarm monitor should report a valid access, displaying cardholder information (if that feature is available). Continue holding the door open. Depending on how the door is configured, a door held alarm should report to the system after 30-60 seconds.
4. Close the door, the door held alarm should clear.

NOTE
Some systems have an alternate wiring configuration which does not generate a door forced open or door held open alarm. If your system is configured in this manner, contact the Denver Security Division for alternate procedures.

[Magnetic Lock Functional Test]

1. With door in the secure position (closed), try to open the door. (Most magnetic locks require a pressure greater than 500 pounds to defeat.) The door must remain closed and not activate the door contact.
2. Using a valid card, gain access to the door by presenting it to the card reader. Alarm monitor should report a valid access, displaying cardholder information.
3. The magnetic lock should release, and the door should open normally.
4. Continue holding the door open. If the magnetic lock is also configured for door status indication, a door held alarm should report to the system after 30-60 seconds.
5. Allow door to close. Do not interfere with the natural action of the door closing. When the door closes, the magnetic lock should activate, and the door held alarm should clear. Select and acknowledge the door held alarm. The alarm should clear.
6. Push on door again and verify it remains secure.

[Electronic Strike Function Test]

1. With the door in the secure position (closed), try to open the door. The door must remain closed and not activate the door contact.
2. Using a valid card, gain access to the door by presenting it to the card reader. Alarm monitor should report a valid access, displaying cardholder information.
3. The electronic strike or latch should release, and the door should open normally.
4. Continue holding the door open. Depending on how the door is configured, a door held alarm should report to the system after 30-60 seconds.
5. Allow the door to close, do not interfere with the natural action of the door closing. When the door closes, the electronic strike should activate. The door held alarm should clear. Select and acknowledge the door held alarm. The alarm should clear.
6. Push on door again and verify it remains secure.

[Request to Exit (REX) Functional Test]

1. A REX can be motion activated or be mechanically activated.
2. The mechanical REX should instantaneously activate upon being pressed.
3. As personnel exiting through the door, the motion REX should detect movement before the door threshold and grant a request to exit prior to opening the door.
4. The motion detector should detect motion within two steps of entry through the door threshold.

a. If the motion detector does not activate, a door forced open alarm will appear at the alarm monitor's station when the door is opened.

[Motion Detector Function Test]

1. Have personnel stand outside the detection area and walk slowly towards the motion detector.
2. An alarm should be activated when motion is detected while walking through the motion detection area.

[Tamper Switch Functional Test]

1. Open the device, the alarm monitor should receive a tamper alarm.
2. Close the device, the alarm should clear. The alarm monitor may need to select and acknowledge the alarm before the alarm will clear.

9.4.3 Electronic Surveillance

[Fixed, PTZ, and Thermal Camera Functional Test]

Fixed Camera Functional Test

1. Verify that user is able to zoom in/out. (If function capable on fixed cameras.)
2. Close the iris to reduce the light (darkening the image) and open the iris to increase the light (lightening the image). Restore the iris to optimal view upon completion. (If function capable on fixed cameras.)
3. Verify that the user is able to use the manual focus to change the focal point in the image. Auto-focus will re-enable once the camera is moved. (If function capable on fixed cameras.)

PTZ and Thermal Camera Functional Test

1. Verify that video image is clear and presentable.
2. Verify that user is able to pan the camera left and right, tilt the camera up and down, and zoom in/out.
3. Close the iris to reduce the light (darkening the image) and open the iris to increase the light (lightening the image). Restore the iris to optimal view upon completion. (This test may not be applicable on thermal cameras.)
4. Verify that the user is able to use the manual focus to change the focal point in the image. Auto-focus will re-enable once the camera is moved. (This test may not be applicable on thermal cameras.)

[Radar Functional Test]

1. Have a subject walk/drive (if over land), operate a UAS (if over air), or operate a watercraft (if over water) in a restricted area covered by the radar and verify an alarm is received.
2. Once subject is clear of restricted/exclusion area, the alarm should clear. Select and acknowledge the alarm. The alarm should clear.
3. Have a subject walk/drive (if over land), operate a UAS (if over air), or operate a watercraft (if over water) in an unrestricted zone and verify no alarm is received.

[Digital/Network Video Recorder (DVR/NVR) Functional Test]

1. Verify display of video using the DVR/NVR as the video source.
2. Verify configuration settings (e.g., record on motion, schedule, record 24/7, etc.) are properly set according to local configuration requirements.
3. Verify that time stamp is aligned between each camera and the ESS system (if applicable) and that the time stamp is accurate.
4. Verify that video is recording according to configuration settings referenced in Step 2.
5. Select a 5-minute segment of recorded video from the DVR/NVR and export using the following removable media:
    a. CD or DVD
    b. USB
6. Replay the video and verify that the playback is free of static, interference and the image is clear.

9.4.4 Batteries and Power Supplies

[Battery/Battery System and Power Supply/Board Functional Test]

Operational status verified through daily use and load test performed during maintenance cycle.

[UPS systems shall be maintained and tested to manufacturer/design requirements, ensuring it can maintain the OT system operational for a system identified minimum period following a failure of station power.] [UPS testing should be performed based on the manufacturer's requirements; or, if no manufacturer's requirement is available, it shall be tested annually.] For details on UPS battery maintenance and testing, see FIST 3-6, Storage Battery Maintenance and Principles.

[The input power should be switched off, and the load on the UPS and the duration that load can be supported should be measured every three years.] Consideration should be made to doing an infrared scan of the UPS during this test. If an actual event occurs during a year for which sufficient information was obtained, such an event can substitute for the annual test. See FIST 3-6, Storage Batteries Maintenance and Principles, for more information. During these tests, measure current draw on the batteries and verify the minimum OT system operational period.

9.4.5 Miscellaneous Devices

[Network Component Functional Test]

Operational status verified through daily use.

[Computer Function Test]

Operational status verified through daily use.

9.4.6 Vehicle Barriers

[Vehicle Barrier Function Test]

Verify barrier cycle up and down times to be within manufacturer's specifications (Refer to owner's manual). Ensure all means to operate are working correctly. Verify manual and automatic activation are functional.

9.4.7 Software

Testing actions should be performed to ensure that the system software performs properly. Normally, the most critical time to perform these actions is when the system is changed. For some control functions, changes may cause a noticeable variation in plant or generator control performance. During the Software functional testing the licensing should be checked and verified if support agreements are active and up to date. This can be accomplished by contacting the manufacturer and providing the Dongle ID, Software license code or software serial number.

[Functional testing of the OT system must be performed to verify proper operation after OT system software changes have been made.] Testing of software operation should be performed on a separate (nonproduction/test) system wherever possible. Testing should include software and firmware updates to RTUs, PLCs, cameras, and other intelligent electronic devices before they are deployed on the production device(s). Testing should confirm proper operation for a minimum of a 24-hour period. Ensure firmware and software updates come directly from the vendor or another trusted resource.

9.4.7.1 *Failure Mode Tests*

Many OT systems provide redundancy and/or distribution of software functions to overcome failures. Failure mode tests identify potential errors and defects that lead to waste, defects or harmful outcomes for the customer and provide risk mitigation strategies. **[Failure mode tests must be identified and performed on primary systems to ensure failures can be overcome.]** These tests should be performed when the systems are placed in service and when configuration changes warrant retesting. (Where primary systems are listed in Section 1.3)

9.4.7.2 *Critical Operations Functional Tests*

[Critical functions will be identified and tested for each OT system.] For example, generation control functions may be considered critical. Facilities should determine and document what is considered a critical function. Performance measures and monitoring normally are built into

these critical functions. Tests should be identified and performed to verify proper operation when changes occur that affect the performance of these functions.

OT systems should have several parameters that can be monitored, that can be used to measure the general health of the system, and that can send an alarm when failures occur. Critical hardware and software should be monitored through an independent process to measure and assess the general health of any monitored condition. The appropriate alarms should be defined to indicate failures to operations staff.

9.4.8 Communications

Communication equipment and error logs should be monitored on a periodic basis to make sure performance is maintained. Procedures should be available to monitor communication system errors so any increased number of errors can be investigated. Bandwidth also should be monitored to determine if system performance is degrading. When degradation is detected, it should be tested and corrected. Communication system hardware also should be maintained per manufacturer requirements.

It is critical to perform testing on the communications equipment used for the OT system. This includes telecommunications equipment and channels required for correct operation of the OT system. It also includes testing equipment used to convey both remote control action and the data used for remote monitoring. **[In addition to the federally mandated testing of transmission equipment utilizing licensed frequencies, unmonitored analog OT system communication requires communication equipment testing upon commissioning, 3 months thereafter (Monitored 5 years), and after equipment modifications.]** The 5-year frequency is determined to coincide with the 5-year DOI inspection frequency.

[Test radio, telephone, satellite, and cellular systems used for voice communication monthly by establishing a voice contact, verifying clear reception, and logging the result.]

A communication system is considered unmonitored unless monitoring and alarming of the function of the communication system is performed by such means as continuous built-in self-monitoring or periodic check-back tests, guard signals, or channel messaging functional indication. Real-time monitoring of the communication alarm signal also is required.

Communication equipment testing: Proper implementation of OT system communications requires a well-defined and coordinated test plan for evaluating the performance of the overall system during the required maintenance intervals. Testing should proceed from the bottom up, beginning at the component level and continuing until the overall system is tested. The employees performing the tests need to have full knowledge of the intent of the scheme, isolation points, simulation scenarios, and restoration to normal procedures or manufacturer’s requirements. Often, this may include coordination with other organizations, to ensure that the communication system is fully tested. Testing the system will verify the overall performance of

the communication schemes, including logic, signal quality, and overall performance to validate the OT system performance.

During the initial commissioning or following major modifications, it is critical to verify that the system operates as designed. The commissioning test also is vital to establish a benchmark of field performance to which future tests will be compared. Verification of the communication system may involve checking signal levels, signal-to-noise ratios, or data error rates. During these tests, the lost-packet count should be monitored, if available. The lost-packet count can be a good indication of channel health. Packets typically are lost due to corruption caused by noise, channel switching, channel fading, or clocking issues if the communication system is not correctly configured. These tests will need to be well documented to ensure the system is tested for different operating and tripping situations that could lead to failures in protection schemes.

The test should determine if the scheme operates correctly or if the scheme has subtle and/or noncritical problems. All problems found during testing should be addressed to determine changes that can be made to eliminate these issues. Trending data over time will help to determine if degradation of the system has occurred, which also can help to determine component failure within the system. If segmented testing is necessary, it is critical to ensure that the zones of testing overlap to verify that the entire system is correctly tested.

In addition to planned testing, utilizing in-service operational data can provide valuable information that can be used to document system performance. Documenting faults and system events can be used to validate performance the entire communication system or any of its parts. Event, oscillograph, and OT system records can be used to verify recently exercised elements of the protection scheme, including communication elements.

[Annually check system enclosures to ensure that it is in good overall condition and maintain according to actions identified in Section 9.3.1.1] Remove any dust or debris and correct any damage as soon as possible.

Data exchange agreements with partner entities (e.g., memorandum of understanding, contracts, etc.) should be prepared where necessary. These agreements also may have requirements for monitoring, security arrangements, and contact procedures in the event of operational or security problems.

10.0 Troubleshooting and Repairs

Repair and troubleshooting methods are an important element in performing proper OT system maintenance. Problems may involve either hardware or software failures. It is generally difficult to detect and repair problems until they occur. As OT systems and their real-time components are complex, a particular failure may not occur until the system has been operational for days,

weeks, or even a longer period. Therefore, detection and identification of system problems become critical. Failure event reporting for SCADA should follow FIST 6.3.

10.1 Remedial Actions for Operations Staff

Initial failure responses often are performed by OT system operations staff. When possible, failures should be planned for, and appropriate remedial action procedures (SOPs) to be used by the operations staff should be developed, documented, and tested. **[OT system remedial action procedures must be documented and reviewed at least annually.]**

10.2 Troubleshooting Procedures

A set of troubleshooting procedures must be developed to diagnose problems when they occur. These procedures must be known to operations staff, when applicable, and software maintenance staff. In some cases, it may be important to leave system conditions in the failure state until OT system support staff can accurately diagnose the problem. These procedures must be understood and clearly documented. These troubleshooting procedures should be reviewed with all affected staff members prior to implementation**. [A troubleshooting library (consisting of trouble tickets, corrective maintenance, technical manuals, commissioning documents, drawings, etc.) must be maintained to assist in identifying trends or recurring failures.]**

Troubleshooting tools should be acquired and maintained to detect performance problems and failures. Alarms and failure indications provided by these tools, where it is feasible, should be integrated into the OT system and its software elements. These tools may include software-based monitors, performance monitors, communication monitors, task managers, and system diagnostic tools. The operation of these troubleshooting tools must be clearly documented.

10.3 Failure Response

Goals for timely response to failures should be set for technical support staff. OT system operations staff and maintenance staff should work together to develop procedures and requirements for failure response. General procedures for responding to failures are provided in the contingency plan developed for the OT systems.

10.4 Configuration Management and Backup/Restore

[Each OT system must have a formal configuration management plan]. This plan may contain inventories hardware, software, and system configuration items, baseline configurations, change authorization procedures, and the periodic review process. The version control process may be used to document all changes to the system and allow roll back to previous versions if a

new version installation fails. The version control process also should protect OT system maintenance staff from making changes that are not properly coordinated.

Backup and restore procedures also should be in place and kept current. If a failure of any component occurs, backups should be provided that allow recovery using the most recent system configuration.

On critical systems that have control capability, there should be at least a minimal offline test system or procedures for testing applications offline. The test system should have enough capability to allow for thorough testing of any new configurations before deploying the actual system.

11.0 Technical Resource Documentation

Technical support for Reclamation OT systems is facilitated by good quality documentation and training for operators and support staff to equip them for performing operations and maintenance tasks.

11.1 General

Proper documentation is critical to the performance of operations and maintenance of an OT system. Documentation should be kept in a location that is available to the OT system support staff and/or operations staff as appropriate, including IT support staff for projects where IT support staff augment the OT system support staff. Documentation should be kept current; and as changes to the OT system occur, documentation should be updated to reflect those changes. As the documentation for the OT system may consist of sensitive materials, consideration should be given to marking them in accordance with the requirements of SLE 02-01, Identifying and Safeguarding CONTROLLED UNCLASSIFIED INFORMATION (CUI). The following list is intended as a general guide for documents that are to be maintained for the system. The actual system documentation may be organized differently, but the elements described should be included.

11.2 Manufacturer's Operation and Maintenance Manuals

OT systems generally have both hardware and software components that have been supplied by a manufacturer and delivered with documentation or provided online.

11.2.1 Operation Documents

[Documentation provided strictly for the operators of the OT system must be available.] These documents should describe all the operational features of the OT system, including display definitions, input procedures, and procedures to perform special functions such as tagging. Documentation to support all troubleshooting activities performed by operation staff and the protocol for interaction with maintenance staff should be included.

11.2.2 General System Documentation

[Documentation must be provided that describes maintenance necessary for the entire system.] Normally, OT systems are made up of several components, which might include communications systems, application nodes, display systems, RTUs, etc. The documents referred to here are documents that describe maintenance requirements for the entire system rather than the individual components.

11.2.2.1 *System Overview*

Describes the entire OT system and integration of its components. Interconnection of the system components should be provided.

11.2.2.2 *System Troubleshooting*

Provides guidance on how to detect problems at the system level such as which module might be contributing to a particular problem.

11.2.2.3 *System Start-Up Procedures*

Used to start up and/or shut down the entire system should be documented.

11.2.2.4 *System Periodic Maintenance and Testing Procedures*

Associated with maintenance and testing of common OT system equipment. Periodicities are specified in FIST 4-1B. **[Periodic maintenance and testing procedures for equipment not identified within this manual must also be documented.]**

11.2.3 Hardware Maintenance Documentation

[Hardware manuals (physical, digital copy or list of hyperlinks) for all OT system components must be available for OT system maintenance staff.] System hardware might include computers, displays, printers, switches, routers, modems, front-end processors, remote terminal units, input/output equipment, and plant wiring. Hardware manuals also should be provided for auxiliary equipment used for OT system maintenance such as simulators, separate software development stations, and maintenance monitoring equipment.

11.2.4 Software Maintenance Documentation

Software maintenance documentation is a key element in performing maintenance on any OT system. The two areas of required documentation for software maintenance for the OT system include COTS and custom application software.

11.2.4.1 *COTS Software*

[Documentation must be available (physical, digital copy or list of hyperlinks) to the OT system support personnel for the COTS software or the basic portions of the system that includes operating systems, applications, development tools, drivers, etc.] Normally, this software is directly associated with the equipment hardware and is provided by the manufacturer. This documentation includes the following items listed below.

1. Operating System Software Manuals. The operating system provides the basic operations for the computers that support the OT system. These basic operations include disk management, user management, display drivers, printer drivers, system startup, network management, diagnostics, and system error logs. The manuals provide information about operations, configuration, and maintenance associated with the operating system.
2. Communication Driver Manuals. The COTS manufacturer may supply input/output drivers for the OT system. Software manuals should describe configuration and functional features of these drivers.
3. Software Development Tools. Supporting documentation for the tools used to perform software development such as editors, compilers, build tools, and system debug tools must be available. This includes software development tools for RTUs and other programmable remote-control devices.

11.2.4.2 *Software Applications*

Documentation must be available for the software applications running on the OT system. These applications deal with software functions that are normally associated with the facilities that the OT system controls. Software applications might include unit controls (start, stop, condense, generate, gate control, generation control, etc.), plant generation controls, bus voltage controls, dam gate or valve controls, historical data functions, sequence of events recording, water and power calculations (energy, releases, inflows, efficiency, etc.), scheduling tools, database tools, trending, alarming, equipment tagging, etc. For each application, software maintenance documentation listed below must be available.

11.2.4.2.1Design Documentation

These documents provide information on how the application functions and include overviews, flowcharts, and interface requirements.

11.2.4.2.2User's Manual

Documentation must be provided to describe installation, configuration, and re-build procedures for OT system support staff that are to maintain the system.

11.2.4.2.3Troubleshooting

Each application must have documented procedures for diagnosing potential problems, errors, and/or alarms. Debug procedures also must be documented.

11.2.5 System Drawings

[System drawings, to include network drawings, must show the current OT system interface points to plant and unit control equipment.] Interface points could include discrete or contact inputs, contact outputs, analog input/output (I/O), and digital I/O. These interface points are used to monitor alarms, monitor equipment status, and perform control. Interface points also may include data interfaces to intelligent devices such as flowmeters, energy meters, governors, regulators, and digital relays.

11.3 Documentation Storage

Documents associated with the OT system, including, but not limit to, reports, logs, media, and manuals, should be stored in appropriate locations. Such locations should be appropriate for each document. Storage in the same location as the OT system should not impede operation and maintenance of the OT system. The documents should be stored in a neat and orderly manner, with sufficient labeling, so that a given document can be readily located.

Definitions

Approved: Acceptable to the authority having jurisdiction.

Access Control System (ACS) – Systems used to monitor, grant, deny, and audit access to ensure that only those individuals with proper access are granted entry and that unauthorized access attempts are denied and recorded. For the purpose of this PEB, access control systems refer to electronic systems.

Annually – Twelve months from the previous occurrence.

Arm – The act of changing a sensor from a standby state, to an active reporting state, thereby requiring acknowledgement/response, in accordance with established protocol.

Authentication – Process of verifying a person's identity by physical or electronic means. Authentication is typically determined by three factors: who you are, what you know, and what you have. For example, who you are is biometrics (fingerprint, retinal scan, etc.), what you know is information you have (PIN, password, etc.), and what you have is some possession that only you should have (PIV card, key fob, etc.).

Card Reader – An electronic device which receives data from an identity card by magnetic strip, proximity antenna, or smart chip. The data is relayed to a processing device which either denies or grants access based on authentication data stored on the processor. 5

Electronic Access Control and Surveillance System (EACSS) – A comprehensive system that provides access control, intrusion detection, and video surveillance; comprised of the Electronic Security System (ESS) and the Video Surveillance System (VSS). EACSS can also be known as a Physical Access Control System (PACS).

Electronic Access Control or Monitoring Systems (EACMS) - Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.

Electronic Security System (ESS) – Controls access, detects intrusions, monitors alarms, generates reports, and audits system use through the use of sensors, control hardware, and management software/hardware.

Intrusion Detection System (IDS) – Detects and reports unauthorized access into the facility, through the use of sensors such as BMS, motion detectors, and radars.

Operational Technology (OT) - Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems or devices detect or cause a direct change through the monitoring or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.

Personal Identity Verification (PIV) Card – A federal smart card that contains the necessary data for cardholders to be granted access to federal facilities and information systems which assures appropriate levels of security for applicable federal applications.

Physical Access Control System (PACS) – Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

Physical Security System (PSS) – A system of devices and protocol used to safeguard/protect personnel, resources, and or locations.

Video Surveillance System (VSS) – Provides detection and assessment capability, as well as video archiving of intrusion events. This is achieved through the use of fixed cameras, pan-tilt-zoom (PTZ) cameras, thermal cameras, and digital/network video.
.