EPE OT Cyber Architecture Guidelines

El Paso Electric — Operational Technology Cyber Security

1. Purpose

The purpose of this document is to define the cyber architecture, security controls, and integration requirements that apply to all Operational Technology (OT) systems owned, operated, or supported by El Paso Electric (EPE). It provides a clear and authoritative set of guidelines for vendors, system owners, and internal project teams when onboarding new OT systems, integrating existing systems, or providing vendor support to EPE OT environments.

This document is intended to be used during procurement, design reviews, change control, and operational handoff for OT systems. By standardizing access, segmentation, monitoring, and vendor integration practices, EPE reduces cyber risk to the Bulk Electric System (BES), supports compliance with the NERC Critical Infrastructure Protection (CIP) Reliability Standards, and ensures that every OT system meets the company's standards for security and operational integrity.

2. Scope

This document applies to all OT systems, industrial control systems (ICS), supervisory control and data acquisition (SCADA) systems, protection and control devices, and supporting network infrastructure that are owned, operated, or accessed on behalf of EPE.

It applies to:

- New OT systems, endpoints and applications being onboarded into EPE.
- Material changes, upgrades, or re-platforming of existing OT systems.
- Vendor-hosted appliances, virtual appliances, or remote services that integrate with EPE OT systems.
- Integrations between EPE OT systems and EPE IT systems, third parties, or cloud services.
- Vendor remote support sessions into EPE OT environments.

It does not apply to:

- Corporate IT systems hosted in the EPE Corporate Data Centers (covered by the EPE Data Center Architecture Requirements).
- Mobile devices, or office productivity systems.
- Systems with no connectivity to EPE OT networks.

Any exceptions to this guideline would be reviewed and, if warranted, approved on a case-by-case basis by EPE.

3. Definitions and Acronyms

Term	Definition
BCSI	BES Cyber System Information.
BES	Bulk Electric System.
CIP	Critical Infrastructure Protection (NERC Reliability Standards).
EAP	Electronic Access Point — a network access point into an Electronic Security Perimeter.
EACMS	Electronic Access Control or Access Monitoring System.
ESP	Electronic Security Perimeter — the logical boundary surrounding a network of BES Cyber Systems.
ICS	Industrial Control System.
IDS	Intrusion Detection System.
IRA	Interactive Remote Access — user-initiated access to a Cyber Asset through a routable protocol.
SRA	Secure Remote Access — Secure intermediate system used to broker administrative access into a protected environment.
MFA	Multi-Factor Authentication.
MFT	Managed File Transfer.
NERC	North American Electric Reliability Corporation.
OT	Operational Technology — hardware and software that detects or causes change through direct monitoring and control of physical devices, processes, and events.
PACS	Physical Access Control System.
PAM	Privileged Access Management.
PCS	Process Control System.
RACI	Responsibility Assignment Chart.
RBAC	Role-Based Access Control.
SCADA	Supervisory Control and Data Acquisition.
SIEM	Security Information and Event Management.
TCA	Transient Cyber Asset.
TLS	Transport Layer Security.

Term	Definition
VPN	Virtual Private Network.

4. Roles and Responsibilities

The following table summarizes the high-level responsibilities for OT systems within EPE. Specific projects may extend this RACI in their design documentation.

Role	Primary Responsibilities
OT/EMS Operations	Owns and operates OT and EMS systems supporting BES operations. Approves architecture for OT systems and authorizes operational changes.
OT Infrastructure	Owns shared infrastructure used by OT systems hosted in OT Data Centers, including virtualization, storage, and backup. Coordinates with OT Operations on change windows and platform standards.
Network Operations	Owns the EPE network architecture, including OT network segmentation, firewall rule management, VPN concentrators, and Electronic Access Points.
OT Cyber Security	Owns security architecture, identity, vulnerability management, SIEM, EDR, and NERC CIP compliance for OT systems. Approves exceptions to controls defined in this document.
Application / System Owner	Business unit accountable for the OT application or system and its lifecycle, including vendor management, configuration baselines, and acceptance of residual risk.
Vendor	Delivers documentation, supports the OT system, provides patches and updates, completes EPE's supply chain risk assessment, and meets the requirements defined in this document.

5. Key Security Controls (CIP-Aligned)

This section defines the baseline cyber security controls that apply to OT systems at EPE. Controls are aligned EPE's Cyber Security policies and the NERC CIP Reliability Standards (primarily CIP-003, CIP-004, CIP-005, CIP-007, CIP-009, CIP-010, and CIP-013). All OT systems must meet these controls as the minimum baseline; additional controls may apply based on impact rating and OT Cyber Security review. Any exceptions to these requirements must be formally requested by Vendor, documented, and approved by EPE.

5.1 Access Control

Access to EPE OT systems is restricted to authorized individuals with a documented business need. All access — employee, contractor, and vendor — is authenticated, authorized, and accountable to a named individual.

- Vendor management — Vendor shall communicate new resource assignments and resource terminations to EPE for authorization approvals and revocations.
- Vendor remote access — All vendor access to OT systems shall be formally approved in advance, granted on a time-bound basis aligned to a specific work order or incident, and fully logged. Standing vendor access is not permitted.
- Multi-Factor Authentication — MFA is required for all interactive remote access to OT systems, including vendor remote support, employee remote administration, and any access that traverses an Electronic Security Perimeter.
- No shared or vendor-managed credentials — Each user shall authenticate with a unique, personally identifiable account. Shared accounts, group accounts, and vendor-managed credentials are prohibited for interactive user authentication. Local accounts are reserved for emergency or break-glass scenarios and are governed by the EPE break-glass account policy.
- Interactive user authentication shall use EPE-managed identity (Active Directory) with Single Sign-On where the OT system supports it. Where it does not, the EPE PAM platform shall broker credentials and session access.
- Role-Based Access Control shall be applied. Role definitions, group membership, and mappings to OT system privileges must be documented and reviewed at least annually.
- Default accounts (root, administrator, sa, admin) shall be renamed where possible, have credentials rotated, and be restricted from utilization for user interactive access.
- Access reviews of all individuals with authorized electronic or unescorted physical access to BES Cyber Systems shall be performed at least every fifteen calendar months in alignment with CIP-004.

5.2 Network Security

OT systems are protected by network architecture that enforces strong segmentation, limits exposure, and brokers all external connectivity through controlled access points. The OT network is treated as a distinct security zone separate from corporate IT and from the Internet.

- OT/IT segmentation — The OT network is logically segmented from the corporate IT network. Traffic between OT and IT must traverse an EPE-managed firewall, and only explicitly approved flows are permitted. Flat layer-2 communication between OT and IT is not permitted.
- Deny-by-default firewall rules — All firewalls protecting OT environments enforce a default-deny posture. Every inbound, outbound, and east-west flow must be explicitly approved, documented with business justification, source, destination, port, and protocol, and reviewed periodically.
- Outbound-only connectivity to vendor and cloud — Where OT systems require communication with vendor or cloud services, the connection shall be initiated outbound from the OT environment to the vendor endpoint. Inbound connections initiated from the Internet or from vendor networks directly into OT are not permitted.

- Electronic Security Perimeters shall be established around BES Cyber Systems in accordance with CIP-005, with all external routable connectivity passing through documented Electronic Access Points.
- Interactive Remote Access into the ESP shall use the EPE-managed VPN and Intermediate System (SRA). Direct routable access from outside the ESP to a BES Cyber System is prohibited.
- Wireless access, cellular modems, and out-of-band management connections directly into OT environments are not permitted without prior written approval from EPE's OT Cyber Security and Network Operations groups.
- Network diagrams identifying ESP boundaries, EAPs, and all external connectivity shall be maintained as current and made available to EPE.

5.3 Monitoring and Visibility

OT environments must be observable so that anomalous activity is detected, investigated, and responded to in a timely manner. Logging is collected at the network, system, and session levels and forwarded to a central platform for correlation and analysis.

- Log collection — VPN, firewall, SRA, interactive remote session, and endpoint logs shall be collected for all access into OT environments. Logs include authentication events, authorization decisions, malicious code detection, session start and end, commands executed where supported, and configuration changes.
- SIEM forwarding — Logs shall be forwarded to the EPE SIEM in near real time using a recognized format (Syslog RFC 5424, Windows Event Log, CEF, or a vendor-published JSON schema). Where direct forwarding from an OT device is not feasible, an EPE-managed collector shall be used.
- Periodic review for anomalies — OT-relevant logs shall be reviewed on a defined cadence for indicators of compromise, policy violations, and unusual access patterns. Findings shall be tracked through the EPE security incident response process.
- Security event monitoring of BES Cyber Systems and associated EACMS shall meet the detection and alerting requirements of CIP-007 R4.
- Local log retention shall meet the longer of EPE policy and applicable regulatory requirements (90 days or longer).
- Vendor-hosted or vendor-supplied appliances that integrate with EPE OT shall expose security and access logs in a format suitable for SIEM ingestion. Vendors that cannot expose required logs require a documented compensating control approved by OT Cyber Security.

5.4 Device and System Security

OT devices and systems are deployed and operated with hardened configurations, controlled change processes, and disciplined patch management. Vendors and project teams are expected to design their solutions to fit within these practices rather than introducing parallel processes.

- Hardened configurations — OT devices and systems shall be deployed against a documented hardening baseline aligned with recognized standards (e.g., CIS Benchmarks, DISA STIGs, vendor security guides). Default credentials shall be changed prior to placing the device in service. Unused services, ports, and protocols shall be disabled, in accordance with CIP-007 R1.
- Patching and update process — A defined process governs the evaluation, testing, and deployment of security patches and firmware updates for OT systems. Vendors shall publish security patch advisories and provide patches in a timeline consistent with the severity of the issue addressed. Security patches shall be evaluated for applicability within 35 calendar days of release in alignment with CIP-007 R2.
- Controlled changes via SRA — All interactive administrative and configuration changes to OT systems shall be performed from an EPE-managed SRA or PAM-mediated session. Direct administrative access from a user workstation is not permitted. If required, Vendor laptops (TCAs) may be used if approved by OT Cyber Security and compliant with EPE's Vendor TCA approval procedures.
- Baseline configurations shall be documented per CIP-010 R1 for each in-scope Cyber Asset, including operating system, installed software, custom software, logical network accessible ports, and security patch level.
- Changes that deviate from the baseline shall follow EPE's Configuration Change Management process and produce evidence suitable for CIP-010 audit.
- OT systems shall support EPE-approved endpoint security capabilities, including EDR, vulnerability scanning, configuration management, and application control where technically feasible. Exceptions and compensating controls shall be documented, reviewed annually, and approved by OT Cyber Security.
- File transfers — Vendors shall use EPE's Managed File Transfer solutions for any file transfer needs to and from OT environments, as applicable.
- Removable media use on OT systems is restricted. If required, devices must be scanned in accordance with the EPE Removable Media Policy prior to use in OT Systems.
- Documentation of compliance with the required cyber security controls will be done using OT's New Cyber Asset Onboarding checklist (Appendix I).

5.5 System Reliability and Recovery

OT vendors and project teams shall design solutions to support reliable operation and timely recovery. System designs must reduce single points of failure, include appropriate redundancy, and define recovery procedures that align with EPE OT's operational and CIP-009 requirements.

- Redundancy and fault tolerance — Critical components shall be designed with redundancy or documented compensating controls to minimize operational impact from equipment, network, or application failures.
- Backup and recovery procedures — Vendors and project teams shall document backup, restoration, and recovery procedures, including roles, dependencies, recovery sequence, and validation steps.

- Testing and evidence — Recovery capabilities shall be tested on a defined cadence where feasible, and evidence of testing, results, and corrective actions shall be retained for operational and compliance review.

6. Vendor Integration Requirements

Vendors that supply, host, or remotely support OT systems for EPE shall integrate into EPE's OT environment under the requirements in this section. These requirements apply in addition to the security controls in Section 5 and to the broader procurement and supply chain risk requirements of CIP-013.

- No direct inbound access to EPE OT systems — Vendors shall not initiate inbound connections from vendor networks or the Internet directly into EPE OT environments, in alignment with CIP-003 and CIP-005 requirements.. Vendor-provided always-on tunnels, vendor-managed VPNs terminated inside the ESP, and vendor cloud services that pull from inside the ESP are not permitted.
- Access via EPE-managed VPN and SRA — All vendor interactive access to OT systems shall be brokered through the EPE-managed VPN concentrator and the EPE-managed SRA (Intermediate System). The SRA enforces multi-factor authentication, session recording, and session time limits, and is the only authorized launching point for interactive sessions into the ESP. Vendor remote access sessions shall be time-bound to a specific work order, change, or incident, and shall be terminated by EPE upon completion of the work.
- Documented ports, protocols, and patch practices — Vendors shall provide documentation of all required network ports and protocols, the patch and update practices applicable to their product (including cadence, testing, and rollback), and the security configuration baselines they support. This documentation is required prior to onboarding and shall be maintained as the product evolves.
- Support for logging and monitoring integration — Vendors shall support integration of their product with EPE's centralized logging and monitoring platforms, including forwarding security-relevant events to the EPE SIEM. Where direct integration is not technically feasible, vendors shall propose a compensating approach for OT Cyber Security review.
- Vendors of systems in scope for NERC CIP must complete EPE's supply chain risk questionnaire and provide evidence supporting CIP-013 requirements, including software integrity and authenticity, vendor remote access controls, and vendor incident notification.
- Vendor-supplied software and firmware shall be obtained from the vendor through a verified channel, and integrity (e.g., hash verification, code signing) shall be validated prior to installation in alignment with CIP-010 R1.6.
- Vendors shall notify EPE of vendor-identified security incidents and vulnerabilities affecting products in use at EPE in accordance with the executed contractual notification terms.

- Vendor personnel with authorized electronic or unescorted physical access to BES Cyber Systems are subject to the personnel risk assessment, and cyber security training provisions of CIP-004.

7. NERC CIP Alignment

The controls defined in this document are designed to align with the NERC CIP Reliability Standards applicable to BES Cyber Systems. The following mapping summarizes the primary CIP standards that motivate each control area. Specific applicability for any given system is determined by OT Cyber Security.

Standard	Coverage in this Document
CIP-002 — BES Cyber System Categorization	System owners and OT Cyber Security categorize OT systems and determine applicability of the controls in this document.
CIP-003 — Security Management Controls	Electronic access controls for Low Impact External Routable Connectivity (LERC) and Dial-up Connectivity. (Sections 5.2, 6).
CIP-004 — Personnel and Training	Access authorization, access reviews, training, and personnel risk assessments for individuals with electronic or unescorted physical access (Sections 5.1, 6).
CIP-005 — Electronic Security Perimeters	ESP definition, Electronic Access Points, Interactive Remote Access via EPE VPN and Intermediate System (Sections 5.2, 6).
CIP-007 — System Security Management	Ports and services, security patch management, malicious code prevention, security event monitoring, system access controls (Sections 5.1, 5.3, 5.4).
CIP-009 — Recovery Plans	Recovery plan requirements in support of the continued stability, operability, and reliability of the BES. (Section 5.5)
CIP-010 — Configuration Change Management and Vulnerability Assessments	Baseline configurations, change management evidence, software integrity verification (Sections 5.4, 6). TCA, Removable media, vulnerability assessments.
CIP-011 — Information Protection	Handling of BES Cyber System Information generated, transmitted, or stored by OT systems and vendor integrations.
CIP-013 — Supply Chain Risk Management	Vendor supply chain risk assessment, software integrity, vendor remote access, vendor incident notification (Section 6).

8. Documentation Requirements

Each OT system within scope of this document must be supported by a documentation package owned jointly by the System Owner and Vendor. The package is required prior to go-live and must be maintained throughout the system's life.

- Solution architecture document, including logical and physical diagrams and the location of the system relative to ESP boundaries.
- Network design package: ports, protocols, flows, IP plan, DNS entries, and identification of Electronic Access Points.
- Identity and access design: authentication method, MFA approach, RBAC role mappings, vendor access workflow.
- Logging and monitoring design: log sources, formats, transport, and SIEM integration.
- Onboarding checklists, configuration baselines, and hardening evidence. Patching and upgrade procedures, with rollback steps and CIP-007 and CIP-010 evidence approach.
- Vendor remote access procedure and architecture, including approval workflow, session brokering, and termination.
- Vendor software development practices, supported OS/software matrix, and data handling procedures.
- Vendor support and escalation contact list, including security incident notification path.
- Supply chain risk evidence (CIP-013) including software integrity verification approach.

9. EPE Preferred technology

- Cisco networking solutions
- HP Enterprise Servers and Workstations
- VMware virtualization technology
- Microsoft Windows 11 and Windows 2025 OS
- Microsoft Office 2024
- RHEL 9
- Ivanti EPM
- Syslog
- Carbon Black App Control and EDR
- SNMPv3 for Network Performance Monitoring
- RSA SecurID for MFA
- Veeam Backup and Replication

10. Review and Revision History

Date	Version	Revised By	History
8/20/2026	1.2	Y. Benavides	Updated applicability scope to broaden exceptions to systems with no connectivity to EPE OT networks. Added statement for general scope exceptions. Modified OT endpoint requirement language in section 5.4 to include exceptions and compensating measures documentation requirements.
7/15/2026	1.1	OT CyberSecurity and NCG	Updated Glossary, CIP standard alignment, requirements, and preferred technology.
5/29/2026	1.0	N. Prieto	Document creation. Initial publication of EPE OT Cyber Architecture Guidelines covering Access Control, Network Security, Monitoring and Visibility, Device and System Security, and Vendor Integration Requirements; aligned with NERC CIP.

Appendix I

See below

CHECKLIST FOR ADDING NEW BES CYBER SYSTEM DEVICE TO ESP

The EMS Engineering Staff will complete the following checklist and associated TFE Form, then attach to the EMS Change Control system anytime a new BES Cyber System is added to the ESP.

GENERAL INFORMATION

Ticket #	
Date:	
Device Type:	
Cyber Asset Type:	
ESP Designation:	
Host Name:	
Asset Tag:	
BU Asset Tag#	
Serial Number:	
IP Address:	
Default Gateway:	
Preferred DNS:	
Alternate DNS:	
Make/Model:	
OS/Firmware:	
Local Accounts:	

Network listening ports:

CHECKLIST

No	**Does the device require a TFE?** If Yes, stop process contact EMSS Management
No	Hardware Inventory (ADD/Verify asset tag, Details, etc.)
N/A	BIOS Hardening
N/A	Drivers
N/A	Microsoft Office (Optional)
N/A	Rename Default User Account (Administrator, Guest, etc.)
N/A	Delete/Disable Unnecessary User Accounts
N/A	Change Default Passwords on Local User Accounts
N/A	Change Computer/Device Name
N/A	System Update (Service Packs, Security Updates, Hotfixes)
N/A	Install/Configure DomainTime/NTP
N/A	Install/Configure LogRhythm/Syslog
N/A	Install/Configure CarbonBlack/Ivanti/AV
N/A	Install/Configure Solarwinds/NetMonitoring
N/A	Install/Configure Ind. Defender/Tenable.OT
N/A	Perform system hardening (ports and services)
No	Scan with vulnerability scanner tool and mitigate any vulnerabilities found
N/A	Join Device to Proper Domain and OU in AD/ Create DNS A Records for network devices
N/A	Create System Baseline

CIP Documentation:		Comments:
☐	Update Proper List Documentation for Cyber Assets (BCA, EACMS, PCA, Transient)	
☐	Completed TFE Eligibility Form	
☐	Fill out and verify system baseline	
☐	Update ESP Diagram	
☐	Upload evidence to SLL	

Engineer: _____ Reviewed by: _____

Signature: _____ Signature: _____