ATTACHMENT "D"

EPE Network Architecture and Infrastructure Standards

El Paso Electric — Network Operations (Operational Technology / Information Technology)

Table of Contents

EPE Network Architecture and Infrastructure Standards 1

1. Purpose 3
2. Scope 3
   It applies to 4
3. Document Classification and Vendor Use 4
4. Definitions and Acronyms 4
   Recommended additions 5
5. Roles and Responsibilities 5
6. Architecture Principles 6
   Required principles 7
7. Network Domains and Security Zones 7
   Domains 8
8. Reference Architecture Requirements 8
   Reference architecture patterns 9
9. Network Segmentation Standards 9
   Requirements 9
10. Routing, Switching, WAN, and Telecommunications Standards 10
    Requirements 10
11. IP Addressing, Naming, and Asset Identification 11
    Requirements 11
12. Firewall and Traffic Flow Requirements 11
    Requirements 11
13. Remote Access and Vendor Access Requirements 12
    Requirements 12
14. Identity, Authentication, and Privileged Access 13

Requirements 13
15. Monitoring, Logging, and Visibility 13
Requirements 13
16. Device and System Security 14
Requirements 14
17. Cloud, Third-Party, and Vendor-Hosted Integration 14
Requirements 15
18. OT, ICS, SCADA, EMS, ADMS, Substation, Generation, and DER/BESS Requirements 15
Requirements 15
19. NERC CIP and Regulatory Compliance Alignment 16
20. Vendor Integration Requirements 16
Vendor requirements 16
21. Documentation Requirements 17
Required documentation package 17
22. Design Review and Approval Requirements 18
Required review gates 18
23. Change Control and Configuration Management 18
Requirements 19
24. Reliability, Resilience, and Disaster Recovery 19
Requirements 19
25. Physical Infrastructure Standards 19
Requirements 19
26. Preferred Technology Standards 20
Categories 20
Starter requirement 21
27. Exception and Risk Acceptance Process 21
Required exception fields 21
28. Operations Handoff and Lifecycle Management 21
Required handoff items 22
29. Review and Revision History 22

1. Purpose

The purpose of this document is to define the network architecture, infrastructure, security, integration, and documentation standards that apply to all Information Technology (IT), Operational Technology (OT), and supporting network environments owned, operated, integrated with, or accessed on behalf of El Paso Electric (EPE).

This standard provides a clear and authoritative set of requirements for internal project teams, application owners, system owners, engineering teams, cybersecurity teams, and vendors when designing, implementing, modifying, or supporting network-connected systems. It is intended to establish consistent expectations for network segmentation, routing, switching, firewalling, remote access, monitoring, vendor integration, documentation, and operational handoff.

This document shall be used during procurement, project planning, design reviews, implementation, change control, commissioning, and operational handoff for any project that requires connectivity to EPE IT or OT networks. This aligns with the existing OT Cyber Architecture Guidelines, which are intended for procurement, design reviews, change control, and operational handoff of OT systems.

By standardizing network architecture and infrastructure practices, EPE reduces operational and cybersecurity risk, improves supportability, strengthens regulatory compliance, and ensures that future systems are designed to meet EPE's standards for reliability, security, maintainability, and operational integrity.

---

2. Scope

This document applies to all new and materially modified systems, applications, network devices, security appliances, remote access solutions, vendor-hosted services, cloud-connected services, and infrastructure components that connect to, traverse, support, or integrate with EPE networks.

This standard applies to both IT and OT environments, including corporate networks, data center networks, EMS/ADMS environments, SCADA systems, industrial control systems, substations, generation facilities, DER/BESS sites, vendor support connections, and integrations between EPE systems and third-party or cloud environments.

The existing OT Cyber Architecture Guidelines apply to OT systems, ICS, SCADA systems, protection and control devices, and supporting network infrastructure owned, operated, or accessed on behalf of EPE. This broader network standard should retain that OT scope while expanding coverage to include IT, and shared network infrastructure.

It applies to

- New IT or OT systems, endpoints, applications, network devices, or appliances being onboarded into EPE environments.
- Material changes, upgrades, migrations, expansions, or re-design of existing systems.
- New sites, substations, generation facilities, DER/BESS projects, control systems, or telecom-connected facilities.
- Vendor-hosted appliances, virtual appliances, remote services, or cloud services that integrate with EPE networks.
- Integrations between EPE IT systems, EPE OT systems, third parties, vendor environments, or cloud services.
- Vendor remote support sessions into EPE IT or OT environments.
- Network changes that affect routing, segmentation, firewall policy, remote access, monitoring, or compliance boundaries.

---

3. Document Classification and Vendor Use

This document is intended to support both internal EPE project planning and controlled vendor engagement. Portions of this standard may be shared with vendors to communicate EPE's architecture, cybersecurity, documentation, and integration expectations.

Information that exposes sensitive internal network details, including IP address ranges, firewall specifics, security tool configuration, privileged access implementation details, vulnerability information, BES Cyber System Information, or detailed diagrams of sensitive environments, shall be handled according to EPE information protection requirements.

This approach is consistent with the existing OT Cyber Architecture Guidelines, which provide requirements for vendors, system owners, and internal project teams while also supporting NERC CIP and OT security objectives.

---

4. Definitions and Acronyms

The following terms and acronyms are used throughout this document. Project teams and vendors shall use these definitions when preparing architecture diagrams, network designs, access requests, firewall rule requests, asset inventories, and project documentation.

Terms already defined in the **OT Cyber Architecture Guidelines** should be referenced from that document rather than duplicated here. This section only adds broader network, and infrastructure terms needed for this standard.

Recommended additions

Term	Definition
ADMS	Advanced Distribution Management System.
BESS	Battery Energy Storage System.
DER	Distributed Energy Resource.
DMZ	Demilitarized Zone used to broker controlled communications between security zones.
iDMZ	Industrial Demilitarized Zone used to separate enterprise and OT environments.
EDR	Endpoint Detection and Response.
EMS	Energy Management System.
LAN	Local Area Network.
MPLS	Multiprotocol Label Switching.
MPLS-TP	MPLS Transport Profile.
NMS	Network Management System.
OT Network	Network infrastructure supporting industrial control, operational, SCADA, EMS, substation, generation, telecom, or BES-related operations.
SIEM	Security Information and Event Management.
VLAN	Virtual Local Area Network.
VRF	Virtual Routing and Forwarding.
WAN	Wide Area Network.
Zero Trust	Security model based on explicit verification, least privilege, and assumed breach principles.

5. Roles and Responsibilities

The following roles are responsible for the design, approval, implementation, operation, monitoring, and support of EPE network architecture and infrastructure. Specific projects may extend this RACI in project-specific design documentation.

OT-specific roles and responsibilities are defined in the **OT Cyber Architecture Guidelines**. This section identifies additional or expanded responsibilities needed for enterprise network architecture, infrastructure, IT, cloud, project delivery, and operational handoff.

Role	Primary Responsibilities
Network Operations	Owns EPE network architecture standards, routing and switching design, segmentation, firewall rule management, VPN concentrators, Electronic Access Points, network monitoring, and operational support of network infrastructure.
OT/EMS Operations	Owns and operates OT and EMS systems supporting operational and BES functions. Approves OT architecture and authorizes operational changes affecting OT environments. This aligns with the OT role described in the existing OT Cyber Architecture Guidelines.

OT Infrastructure	Owns shared infrastructure used by OT systems, including virtualization, storage, backup, and related platforms supporting OT environments. This role is identified in the existing OT Cyber Architecture Guidelines.
IT Infrastructure / Data Center Operations	Owns enterprise compute, storage, virtualization, data center connectivity, and supporting infrastructure for corporate IT and non-OT hosted systems.
Telecommunications	Owns telecom transport, fiber, WAN, carrier circuits, microwave, MPLS/MPLS-TP, and communications infrastructure supporting IT, OT, substations, generation, and field operations.
Cybersecurity	Owns, reviews and approves security architecture, access models, identity, monitoring requirements, vulnerability management requirements, SIEM, EDR and security exceptions.
Compliance	Reviews applicability of regulatory requirements, including NERC CIP where applicable, and confirms that project documentation supports required evidence retention.
Application / System Owner	Business or technical owner accountable for the application or system lifecycle, vendor coordination, access requirements, data flows, documentation, and acceptance of residual risk. The existing OT Cyber Architecture Guidelines assign lifecycle, vendor management, configuration baseline, and residual risk responsibilities to Application/System Owners for OT systems.
Vendor / Contractor	Delivers required documentation, supports implementation, provides patches and updates, completes required risk assessments, and complies with the requirements defined in this document. The existing OT Cyber Architecture Guidelines assign vendors responsibilities for documentation, support, patches, updates, supply chain risk assessment, and compliance with defined requirements.
Project Manager	Ensures architecture reviews, cybersecurity reviews, documentation deliverables, change control, testing, and handoff activities are included in the project schedule.

6. Architecture Principles

All EPE network designs shall follow a consistent set of architecture principles. These principles apply regardless of whether the project is led by an internal team, vendor, system integrator, construction contractor, or managed service provider.

EPE network architecture shall prioritize safety, reliability, security, maintainability, compliance, and operational supportability. Designs shall avoid one-off implementations that cannot be monitored, patched, supported, or integrated into EPE's operational processes.

All network designs shall be evaluated against four core tenets: **Secure**, **Scalable**, **Simple**, and **Supportable**. These tenets shall guide architecture decisions, technology selection, segmentation models, operational handoff, and long-term lifecycle planning.

The architecture should aligning OT designs with defense in depth, Purdue model concepts, ISA/IEC 62443, NIST SP 800-82, and Zero Trust concepts. For OT-specific cybersecurity controls, NERC CIP alignment, access requirements, monitoring, vendor integration, and OT control baseline details, refer to the **OT Cyber Architecture Guidelines**. This document intentionally avoids duplicating those requirements and focuses on broader network architecture and infrastructure standards across IT, OT, telecom, and shared infrastructure.

Required principles

- **Four-tenet design model** — Network designs shall be reviewed to confirm they are **Secure**, **Scalable**, **Simple**, and **Supportable** before implementation.
- **Segmentation by design** — IT, OT, telecom, cloud, and management networks shall be logically separated based on trust level, function, and risk.
- **Deny by default** — Network access shall be explicitly approved and documented. Unapproved traffic is not permitted.
- **Least privilege** — Users, systems, vendors, and applications shall only receive the access required to perform approved business or operational functions.
- **No unmanaged access paths** — Vendors shall not introduce unmanaged VPNs, modems, cellular connections, remote support tools, or cloud tunnels without formal EPE approval.
- **Documented data flows** — All required communications shall be documented before implementation.
- **Security and monitoring built in** — Logging, alerting, and monitoring requirements shall be included in the design, not added after deployment.
- **Operations handoff required** — No project shall be considered complete until documentation, monitoring, support procedures, and ownership are accepted by the responsible EPE operations team.
- **Exceptions require approval** — Any deviation from this standard must be documented, risk reviewed and approved before implementation.

---

7. Network Domains and Security Zones

EPE network architecture shall be organized into defined domains and security zones. Each domain shall have a documented purpose, owner, trust level, allowed connectivity, standard access method, monitoring requirements, and applicable compliance considerations.

At minimum, network designs shall identify whether the proposed system or connection resides in, connects to, or traverses one or more of the following domains.

Domains

Domain / Zone	Description
Corporate IT Network	Supports enterprise business applications, end-user services, office productivity, corporate identity, and general business operations.
Data Center Network	Supports hosted enterprise applications, shared infrastructure, virtualization, storage, backup, management platforms, and interconnection to other EPE domains.
OT Network	Supports operational systems, ICS, SCADA, EMS, protection and control, generation, substations, and other systems involved in monitoring or control of physical processes. The existing OT Cyber Architecture Guidelines define OT as hardware and software that detects or causes change through direct monitoring and control of physical devices, processes, and events.
EMS / Control Center Environment	Supports systems used for real-time monitoring, control, and operation of the electric system.
ADMS / Distribution Operations Environment	Supports distribution operations, distribution automation, outage management, and related operational functions.
Substation Network	Supports substation automation, SCADA communications, protection and control, engineering access, monitoring, and telecom connectivity.
Generation Network	Supports plant control systems, generation operations, balance-of-plant systems, vendor support, and monitoring.
DER / BESS Network	Supports distributed energy resource and battery energy storage site connectivity, telemetry, control, monitoring, vendor support, and integration to EPE systems.
Telecommunications Network	Supports wide-area communications, fiber transport, MPLS/MPLS-TP, relay communications, field connectivity, and critical communications services.
Industrial DMZ / OT DMZ	Brokers approved communications between enterprise, vendor, cloud, and OT environments.
Management Network	Supports administrative access to infrastructure devices, monitoring, logging, configuration backup, and privileged management.

8. Reference Architecture Requirements

Each project shall align to an approved EPE reference architecture pattern. Where no approved pattern exists, the project team shall develop a proposed architecture and submit it for review by Network Operations, OT Infrastructure Cybersecurity, Telecommunications, and other required stakeholders before implementation.

Reference architectures shall include logical diagrams, physical diagrams where applicable, data flow diagrams, security zone boundaries, firewall locations, Electronic Access Points, remote access paths, monitoring points, and integration dependencies.

For OT-specific diagram requirements, including ESP boundaries, Electronic Access Points, and external connectivity, refer to the **OT Cyber Architecture Guidelines**.

Reference architecture patterns

- Corporate IT application architecture
- Data center hosted application architecture
- IT-to-OT integration architecture
- OT iDMZ architecture
- EMS/ADMS network architecture
- Generation plant network architecture
- Substation network architecture
- DER/BESS site architecture
- Vendor remote access architecture
- Cloud-to-EPE integration architecture
- Network management architecture
- SIEM/logging architecture
- Telecommunications/MPLS architecture
- Disaster recovery architecture
- Firewall segmentation architecture
- Identity and privileged access architecture

---

9. Network Segmentation Standards

EPE networks shall be segmented based on operational function, trust level, regulatory impact, cybersecurity risk, and support model. Segmentation shall be enforced using approved network controls such as firewalls, access control lists, VRFs, VLANs, routing controls, and security zones.

OT segmentation requirements are governed by the **OT Cyber Architecture Guidelines**. This standard references those requirements and applies compatible segmentation principles to broader EPE network environments.

Requirements

- IT and OT networks shall be logically separated.
- Traffic between network zones shall be explicitly approved, documented, and monitored.
- Firewall rules shall follow a default-deny model.

- Direct internet access from OT environments is not permitted unless formally approved.
- Direct vendor access into OT environments is not permitted.
- East-west traffic within sensitive environments shall be restricted based on system function and business need.
- Management traffic shall be separated from user, application, control, and vendor traffic where feasible.
- Security zones shall be shown on project diagrams.
- For BES Cyber Systems, Electronic Security Perimeters and Electronic Access Points shall be identified where applicable.

---

10. Routing, Switching, WAN, and Telecommunications Standards

Network designs shall follow EPE-approved routing, switching, WAN, and telecommunications standards. Designs shall support reliability, path diversity, operational visibility, secure management, and long-term maintainability.

Projects shall document all routing, switching, WAN, telecom, and circuit requirements before implementation. Documentation shall include VLANs, VRFs, subnets, routing protocols, static routes, WAN paths, telecom dependencies, redundancy requirements, and failover behavior.

Requirements

- Use EPE-approved routing and switching platforms.
- Document all VLANs, VRFs, routed interfaces, subnets, and WAN paths.
- Avoid unnecessary Layer 2 extension across sites, security zones, or trust boundaries.
- Redundant paths shall be physically and logically diverse where required by the application, site, or operational function.
- Routing changes shall be reviewed by Network Operations before implementation.
- QoS requirements shall be documented for latency-sensitive or critical traffic.
- Telecom dependencies shall be identified during design.
- Protection, control, SCADA, voice, telemetry, and management traffic shall be classified and prioritized where applicable.
- Out-of-band management shall be approved, documented, and secured.
- Network designs shall avoid undocumented backdoor connectivity.

---

11. IP Addressing, Naming, and Asset Identification

All network-connected systems shall follow EPE-approved IP addressing, naming, and asset identification standards. Project teams and vendors shall not assign IP addresses, hostnames, VLANs, DNS entries, or network identifiers without coordination with the appropriate EPE infrastructure owner.

For OT systems, the existing OT Cyber Architecture Guidelines require documentation of network design information, including ports, protocols, flows, IP plan, DNS entries, and identification of Electronic Access Points.

Requirements

- IP addresses shall be assigned by EPE Network Operations.
- IP plans shall identify subnet, gateway, VLAN, VRF, security zone, location, and system owner.
- Hostnames shall follow EPE naming conventions.
- DNS and reverse DNS requirements shall be documented.
- Network devices shall be entered into EPE asset inventory and monitoring platforms.
- Vendors shall provide make, model, serial number, firmware/software version, MAC address, IP address, location, and support information for all supplied devices.
- Cyber asset identification requirements shall be followed where applicable.
- Asset records shall be updated before go-live and during material changes.

---

12. Firewall and Traffic Flow Requirements

All communications across EPE security zones shall be documented and explicitly approved. Firewall rules shall be based on least privilege and shall include business justification, source, destination, port, protocol, application, owner, and review requirements.

For OT-specific firewall posture, traffic flow approval, and periodic review requirements, refer to the **OT Cyber Architecture Guidelines**.

Requirements

- Firewall rules shall be deny-by-default.
- “Any-any” rules are prohibited unless formally approved as an exception.
- Temporary rules shall have an expiration date.
- Firewall requests shall include:
    - Business justification
    - Source IP/subnet
    - Destination IP/subnet
    - Port and protocol

    - Application or service name
    - Direction of traffic
    - System owner
    - Security zone
    - Requested duration
    - Logging requirement
- Firewall logging shall be enabled for approved traffic where required.
- Firewall rule changes shall follow EPE change control.
- Enter remarks on the configuration

---

13. Remote Access and Vendor Access Requirements

Remote access to EPE networks shall be controlled, authenticated, authorized, logged, and limited to approved business or operational purposes. Vendor access shall be time-bound, associated with an approved work order, change, support case, or incident, and terminated when the approved work is complete.

For OT-specific vendor remote access requirements, including approval, time-bound access, logging, MFA, and use of EPE-managed access paths, refer to the **OT Cyber Architecture Guidelines**.

Requirements

- Remote access shall use EPE-approved remote access solutions.
- MFA is required for interactive remote access.
- Vendor remote access shall be approved in advance.
- Vendor access shall be time-bound.
- Standing vendor access is not permitted unless formally approved as an exception.
- Shared accounts, group accounts, and vendor-managed credentials shall not be used for interactive access.
- Vendor access into OT shall use EPE-managed VPN and an EPE-managed Secure Remote Access or intermediate system where applicable. The existing OT Cyber Architecture Guidelines require vendor interactive access to OT systems to be brokered through the EPE-managed VPN concentrator and EPE-managed SRA.
- Remote sessions shall be logged.
- Session recording shall be used where supported or required.
- Emergency access shall follow an approved break-glass process.
- Vendor access shall be revoked when no longer required.

---

14. Identity, Authentication, and Privileged Access

Access to EPE systems shall be tied to a named individual and authorized based on role, responsibility, and business need. Privileged access shall be controlled, monitored, and periodically reviewed.

For OT-specific identity, authentication, named individual accountability, and privileged access requirements, refer to the **OT Cyber Architecture Guidelines**.

Requirements

- Each user shall authenticate with a unique, personally identifiable account.
- Shared accounts, group accounts, and vendor-managed credentials are prohibited for interactive user authentication in OT environments under the current OT Cyber Architecture Guidelines.
- MFA shall be required for remote and privileged access where applicable.
- Role-Based Access Control shall be applied.
- Role definitions, group membership, and mappings to system privileges shall be documented.
- Privileged access shall use EPE-approved PAM or SRA capabilities where applicable.
- Default accounts shall be renamed where possible, credentials rotated, and restricted from interactive user access where applicable. The existing OT Cyber Architecture Guidelines include this requirement for OT systems.
- Break-glass accounts shall be documented, protected, monitored, and reviewed.
- Access reviews shall be performed on a defined cadence.

---

15. Monitoring, Logging, and Visibility

Network and system designs shall include monitoring, logging, and visibility requirements as part of the initial architecture. EPE must be able to detect, investigate, and respond to anomalous activity, system failures, unauthorized access, and configuration changes.

For OT-specific logging, monitoring, SIEM forwarding, session logging, and visibility requirements, refer to the **OT Cyber Architecture Guidelines**.

Requirements

- Network devices shall send logs to approved logging platforms.
- VPN, firewall, SRA, session, endpoint, and authentication logs shall be collected where applicable.
- Logs shall be forwarded to the EPE SIEM where required.
- Network devices shall support secure logging protocols where feasible.
- Time synchronization shall be configured for log correlation.

- Monitoring shall include device availability, interface utilization, errors, routing status, environmental status, and security events.
- Vendor-hosted or vendor-supplied appliances that integrate with EPE environments shall expose logs suitable for EPE review or ingestion where required.
- Monitoring onboarding shall be completed before production go-live.

---

16. Device and System Security

Network infrastructure, appliances, and systems shall be deployed using hardened configurations, secure management protocols, controlled patching, and documented baselines. Project teams and vendors shall design solutions to integrate with EPE's security and operational processes.

For OT-specific hardening, patching, baseline, endpoint protection, removable media, and managed file transfer requirements, refer to the **OT Cyber Architecture Guidelines**.

Requirements

- Default credentials shall be changed before production use.
- Unused services, ports, and protocols shall be disabled where feasible.
- Secure management protocols shall be used.
- Configuration baselines shall be documented.
- Configuration backups shall be enabled for network infrastructure where applicable.
- Patching and firmware update procedures shall be documented.
- Vendors shall provide patch advisories, supported software/firmware versions, and rollback procedures.
- Changes that deviate from approved baselines shall follow EPE change control.
- OT systems shall support EPE standard agents such as backup, monitoring, EDR, vulnerability scanning, and configuration management where technically feasible. The existing OT Cyber Architecture Guidelines include this requirement and require vendor exclusions to be documented and reviewed.
- Removable media use shall be restricted and controlled where applicable.
- File transfers into protected environments shall use approved methods. The existing OT Cyber Architecture Guidelines require vendors to use EPE Managed File Transfer solutions for file transfer needs to and from OT environments, as applicable.

---

17. Cloud, Third-Party, and Vendor-Hosted Integration

Cloud, third-party, and vendor-hosted integrations shall be reviewed and approved before implementation. These integrations shall not bypass EPE network segmentation, identity, monitoring, logging, access control, or compliance requirements.

For OT integrations with IT, third parties, vendors, or cloud services, refer to the **OT Cyber Architecture Guidelines**.

Requirements

- Cloud or third-party connectivity shall be documented in the architecture package.
- Data flows shall be documented and approved.
- Internet-facing services shall require cybersecurity review.
- Vendor-hosted systems shall disclose access methods, data handling, logging capabilities, patch practices, and support model.
- Inbound connections from vendor networks or the Internet directly into OT environments are not permitted under the existing OT Cyber Architecture Guidelines.
- Where OT systems require vendor or cloud communication, the connection shall be initiated outbound from the OT environment to the vendor endpoint where applicable. The OT Cyber Architecture Guidelines state this requirement for OT vendor and cloud connectivity.
- Vendor cloud services shall not introduce unmanaged access paths into EPE networks.
- Encryption, authentication, logging, and support responsibilities shall be documented.
- Cloud and third-party integrations shall identify data classification and information protection requirements.

---

18. OT, ICS, SCADA, EMS, ADMS, Substation, Generation, and DER/BESS Requirements

Projects involving OT, ICS, SCADA, EMS, ADMS, substation, generation, DER, BESS, protection and control, or other operational systems shall comply with this network standard and the **OT Cyber Architecture Guidelines**. OT-specific cybersecurity and NERC CIP-aligned control language should be maintained in the OT guideline document rather than duplicated here.

Requirements

- OT systems shall be segmented from corporate IT.
- OT access shall be authenticated, authorized, logged, and limited to approved users.
- OT remote access shall use approved EPE remote access methods.
- OT systems requiring vendor support shall follow the vendor access requirements in this document and the OT Cyber Architecture Guidelines.
- OT systems shall provide required documentation before go-live.

- OT systems shall support required logging and monitoring where technically feasible.
- SCADA, EMS, ADMS, substation, generation, DER/BESS, and protection/control systems shall identify all network flows, protocols, dependencies, and external connections.
- Any system that may impact BES operations shall be reviewed for NERC CIP applicability.
- Projects shall identify whether the system stores, processes, or transmits BES Cyber System Information.

---

19. NERC CIP and Regulatory Compliance Alignment

This document supports EPE's compliance with applicable regulatory, cybersecurity, and reliability requirements. For systems that fall within the scope of NERC CIP, project teams shall coordinate with CyberSecurity and Compliance to determine applicability, required controls, evidence expectations, and documentation requirements.

For OT and BES Cyber System applicability, control mappings, and NERC CIP-aligned evidence expectations, refer to the **OT Cyber Architecture Guidelines**.

---

20. Vendor Integration Requirements

Vendors that supply, host, install, configure, integrate, or remotely support network-connected systems for EPE shall comply with the requirements in this document. These requirements apply in addition to any contractual, procurement, cybersecurity, compliance, or project-specific requirements.

For OT vendor integration, supply chain risk, remote access, logging, incident notification, and CIP-related vendor requirements, refer to the **OT Cyber Architecture Guidelines**.

Vendor requirements

- Vendors shall not establish direct inbound connectivity into EPE OT environments.
- Vendors shall not install unmanaged VPNs, remote access tools, cellular modems, wireless access points, or cloud tunnels without prior written approval.
- Vendors shall use EPE-approved access methods.
- Vendors shall provide documentation of all required ports and protocols.
- Vendors shall support logging and monitoring integration where required.
- Vendors shall provide supported software, firmware, OS, and hardware matrices.
- Vendors shall provide patch, upgrade, rollback, and vulnerability notification procedures.
- Vendors in scope for NERC CIP shall provide required supply chain risk evidence.

21. Documentation Requirements

Each project within scope of this document shall produce a complete documentation package before production go-live. Documentation shall be maintained throughout the lifecycle of the system and updated when material changes occur.

For OT-specific documentation package requirements and OT cyber asset onboarding documentation, refer to the **OT Cyber Architecture Guidelines**.

Required documentation package

- Executive summary of the solution
- Business and operational purpose
- Architecture diagram
- Logical network diagram
- Physical network diagram
- Security zone diagram
- Data flow diagram
- IP address plan
- VLAN and VRF plan
- DNS requirements
- Firewall rule matrix
- Ports and protocols list
- Remote access design
- Vendor access procedure
- Identity and access design
- MFA and RBAC approach
- Logging and monitoring design
- SIEM integration requirements
- Backup and recovery requirements
- Patch and upgrade procedure
- Rollback procedure
- Configuration baseline
- Hardening evidence
- Asset inventory
- Bill of materials
- Rack elevation
- NERC CIP evidence approach, where applicable
- As-built documentation
- Operations handoff checklist

22. Design Review and Approval Requirements

Projects shall complete required architecture, cybersecurity, network, telecom, OT, compliance, and operational readiness reviews before implementation. Reviews shall occur early enough in the project lifecycle to influence design decisions before hardware, software, circuits, contracts, or vendor solutions are finalized.

No system, application, vendor appliance, network connection, firewall rule set, remote access method, or cloud integration shall be placed into production until required reviews are complete, required documentation is accepted, monitoring requirements are implemented, and the responsible EPE operational owner approves handoff.

Required review gates

- Conceptual design review
- Preliminary architecture review
- Detailed design review
- Network Operations review
- Cybersecurity review
- Telecommunications review, where applicable
- Data Center / Infrastructure review, where applicable
- Compliance review, where applicable
- Firewall and traffic flow review
- Remote access review
- Monitoring and logging review
- Change control review
- Post-implementation validation
- Final operations handoff approval

23. Change Control and Configuration Management

All network and infrastructure changes shall follow EPE change control and configuration management processes. Changes shall be planned, reviewed, approved, implemented, validated, and documented.

For OT-specific configuration change evidence and CIP-010 alignment, refer to the **OT Cyber Architecture Guidelines**.

Requirements

- Changes shall have documented scope, reason, risk, implementation steps, validation steps, and backout plan.
- Changes affecting security zones, firewalls, routing, remote access, monitoring, or compliance boundaries require appropriate stakeholder review.
- Configuration baselines shall be updated after approved changes.
- As-built diagrams shall be updated after implementation.
- Change evidence shall be retained where required.
- Emergency changes shall be documented after implementation according to EPE process.
- Vendor-executed changes shall be approved and observed or reviewed by EPE where required.

---

24. Reliability, Resilience, and Disaster Recovery

Network and infrastructure designs shall support the reliability and availability requirements of the systems they serve. Critical business, operational, telecom, and OT systems shall be designed to minimize single points of failure and support recovery objectives defined by the system owner and EPE operations teams.

Requirements

- Critical network paths shall include redundancy where required.
- Redundant components shall not share unnecessary single points of failure.
- Primary and backup communication paths shall be documented.
- Power, rack, cabling, and environmental dependencies shall be reviewed.
- Failover behavior shall be documented and tested where applicable.
- Disaster recovery connectivity shall be included in the design.
- Monitoring shall detect failures of redundant components.
- Operational procedures shall define support, escalation, and recovery steps.
- Maintenance windows shall consider operational and regulatory impacts.

---

25. Physical Infrastructure Standards

Network-connected systems shall comply with EPE physical infrastructure standards for rack placement, cabling, labeling, power, environmental conditions, physical security, and maintainability.

Requirements

- Equipment shall be installed in approved racks, cabinets, rooms, or enclosures.

- Cabinets and enclosures supporting sensitive or operational systems shall be physically secured.
- Cabling shall follow EPE labeling and cable management standards.
- Fiber and copper paths shall be documented.
- Redundant paths shall be physically separated where required.
- Power requirements shall be documented.
- UPS or backup power requirements shall be identified.
- Environmental requirements shall be documented.
- Rack elevations and cable schedules shall be provided before handoff.
- Field equipment shall be labeled and documented for supportability.

---

26. Preferred Technology Standards

Projects shall use EPE-approved technology platforms unless an exception is formally approved. Standardization improves supportability, monitoring, patching, recovery, spare parts management, vendor support, and lifecycle planning.

OT-specific preferred technology baselines are maintained in the **OT Cyber Architecture Guidelines**. This section identifies broader technology categories for enterprise network and infrastructure standardization.

Categories

- Network switching and routing platforms
- Firewall and security platforms
- VPN and remote access platforms
- Server and workstation platforms
- Virtualization platforms
- Operating systems
- Endpoint protection and EDR
- Monitoring and logging tools
- Network performance monitoring
- MFA and PAM platforms
- Backup and recovery platforms
- Configuration management tools
- Time synchronization services
- Approved cabling, optics, and transceiver standards

Starter requirement

Any request to use non-standard technology shall include a business justification, technical justification, risk assessment, lifecycle plan, support model, cybersecurity review, monitoring approach, and exception approval.

---

27. Exception and Risk Acceptance Process

Exceptions to this standard shall be formally documented, reviewed, and approved before implementation. Exceptions shall not be treated as permanent unless explicitly approved as such.

Any exception request shall include the requirement being excepted, reason for the exception, affected systems, business justification, technical justification, risk assessment, compensating controls, duration, owner, and required approvals.

For OT-specific control exceptions and approval requirements, refer to the **OT Cyber Architecture Guidelines**.

Required exception fields

- Requirement number or section
- Description of requested exception
- Business justification
- Technical justification
- Affected system or environment
- Risk description
- Compensating controls
- Requested duration
- Expiration or review date
- System owner approval
- Network Operations approval
- Cybersecurity approval
- Compliance approval, where applicable

---

28. Operations Handoff and Lifecycle Management

Projects shall complete an operations handoff before the system or network connection is considered production-ready. Handoff ensures that EPE teams can monitor, support, troubleshoot, patch, recover, and manage the system throughout its lifecycle.

Required handoff items

- Final approved architecture
- Asset inventory
- As-built network diagrams
- IP address plan
- Firewall rule matrix
- Device configurations or configuration backups
- Monitoring confirmation
- Logging/SIEM confirmation
- Warranty and support contract information
- Patch and firmware process
- Backup and recovery process
- Admin access model
- Final acceptance by operational owner

29. Review and Revision History

Date	Version	Revised By	Summary of Changes
TBD	1.0	G. Olivares	Initial approved publication.
8/5/2026	0.1	G. Olivares	Initial draft of EPE Network Architecture and Infrastructure Standards.