OT COMPLIANCE ALIGNMENT GUIDE

Total Access Control (TAC) for NERC CIP and IEC 62443

How TAC delivers the technical access control, authentication, monitoring, and audit evidence requirements of NERC CIP and IEC 62443 — for the systems that command your OT environment.

Audience	Frameworks	Version
OT CISOs, OT/ICS security architects, NERC registered entities, IEC 62443 candidates, DIB OT contractors	NERC CIP v7+, IEC 62443-3-3	v1.0 — 2026

TAC Scope in OT. TAC controls access to **systems and access paths INTO your OT environment** — HMIs, SCADA servers, engineering workstations, historians, and remote-access tools. TAC sits in the IT/OT DMZ as a reverse proxy, enforcing the boundary between IT and OT zones. TAC addresses the electronic access control, authentication, monitoring, and audit layer.

TAC does **not** touch, configure, or modify OT devices themselves (PLCs, RTUs, IEDs, control system components). It does not perform asset inventory, change management, BES Cyber System categorisation, or address physical security, training, recovery planning, supply-chain risk, or data-at-rest within OT systems. Those are program-level and OT-internal activities addressed by complementary controls in your environment.

Why Access Control Sits at the Center of Both Frameworks

NERC CIP and IEC 62443 use different language and address different industries, but both frameworks reach the same conclusion about OT security: the most consequential controls are at the boundary between IT and OT, not on the OT devices themselves. NERC CIP-005 calls it the Electronic Security Perimeter (ESP). IEC 62443 calls it zones and conduits. The principle is identical — define the boundary, control what crosses it, log every crossing.

Both frameworks also expect strong authentication and access management for the humans and systems that reach OT — engineers, vendors, contractors, IT administrators. NERC CIP-007 specifies system security management including account and password controls. IEC 62443 requires identification, authentication, and use control across every level. These are access control problems, not endpoint problems.

TAC is purpose-built for this layer. It sits in the IT/OT DMZ, enforces identity-, posture-, and policy-based access to every system that commands your OT environment, and produces the audit evidence both frameworks expect — without requiring any change to the OT devices themselves.

Part A: NERC CIP — Standard Mapping

TAC delivers the technical controls behind **CIP-005** (Electronic Security Perimeter) and **CIP-007** (System Security Management), with supporting evidence for **CIP-004** (Personnel and Access Management).

ELECTRONIC SECURITY PERIMETER

CIP-005 — Primary Coverage

REQUIREMENT	HOW TAC DELIVERS
R1 — Electronic Security Perimeter	TAC sits in the IT/OT DMZ as a single-port encrypted reverse proxy, defining and enforcing the ESP boundary. All inbound access to systems inside the OT zone passes through TAC. Other inbound ports are closed at the firewall.
R1.5 — Inbound and outbound access permissions	Per-user, per-system, per-protocol policy enforcement at the proxy. Least-privilege access defined and applied to every connection to OT-adjacent systems. Real-time policy changes take effect without service interruption.
R2 — Interactive Remote Access	All interactive remote access to OT-adjacent systems is brokered through TAC. The **Intermediate System** role required by CIP-005 R2 is fulfilled by TAC's reverse proxy — no separate jump server required.
R2.1 — Encryption of remote access	All TAC-brokered sessions encrypted via TLS 1.2 or TLS 1.3 with FIPS 140-2 compliant cryptographic modules through a single port. No unencrypted remote-access paths into the ESP remain after TAC deployment.
R2.2 — Multi-factor authentication for remote access	FIDO2 / WebAuthn (phishing-resistant), SafeLogin (proprietary), TOTP, push notifications, SMS, OTP, and hardware tokens supported. Third-party MFA integration with Duo, RSA, Swivel, biometric solutions, and others. MFA enforced on every remote-access session, including vendor and contractor access. All MFA methods included in base licence.
R3 — Vendor remote access	Vendor sessions are time-bounded, scoped to specific systems, identity-verified through federation or TAC-managed credentials, and individually logged. Disabling vendor access is immediate and complete — no orphaned access remains.

SYSTEM SECURITY MANAGEMENT

CIP-007 — Primary Coverage

REQUIREMENT	HOW TAC DELIVERS
R1 — Ports and services	By centralising remote access through one encrypted port, TAC reduces inbound exposure across all OT-adjacent systems. Unused ports and services on the ESP boundary close as a natural byproduct of TAC deployment.

REQUIREMENT	HOW TAC DELIVERS
R4 — Security event monitoring	Every authentication attempt, allow/deny decision, session establishment, and policy enforcement event is logged with full attribution. TAC provides native real-time monitoring and alerting; logs are exportable via syslog or API to SIEM for retention and correlation per CIP-007 R4 requirements.
R5 — System access control	Individual user accounts authenticated against your upstream identity provider. Shared accounts are not required. Account inventory, removal of unnecessary accounts, and password policies are enforced through the upstream identity source TAC consumes — TAC does not maintain a separate credential store.
R5.6 — Authentication failure response	Failed authentication attempts are logged and rate-limited at the proxy. Configurable lockout policies prevent brute-force credential attacks against OT-adjacent systems.

PERSONNEL & ACCESS MANAGEMENT

CIP-004 — Supporting Coverage

REQUIREMENT	HOW TAC DELIVERS
R4 — Access management program	TAC enforces the access decisions made by your access management programme: who can reach which OT-adjacent systems, from what devices, at what times. Quarterly access reviews are supported by the TAC audit log.
R5 — Access revocation	Disabling a user at the upstream identity provider immediately revokes that user's TAC sessions and prevents future access. CIP-004 R5 same-day revocation timeline is met by default — no need to wait for next login cycle.

> **NERC CIP Out of Scope.** TAC does not address CIP-002 (BES Cyber System categorisation), CIP-003 (Security Management Controls), CIP-006 (Physical Security), CIP-009 (Recovery Plans), CIP-010 (Configuration Change Management and Vulnerability Assessments), CIP-011 (Information Protection), CIP-013 (Supply Chain Risk Management), or CIP-014 (Physical Security of Control Centers). These are program-level, physical, and organisational activities outside the scope of an access control platform. TAC produces audit evidence (session logs, access changes, ESP boundary configuration) that supports recordkeeping for several of these standards.

Part B: IEC 62443-3-3 — Foundational Requirements Mapping

TAC supports the foundational requirements (FRs) of IEC 62443-3-3 most relevant to access control, authentication, monitoring, and remote access for industrial systems.

IDENTIFICATION, AUTHENTICATION & USE CONTROL

FR 1 & FR 2 — Primary Coverage

REQUIREMENT	HOW TAC DELIVERS
SR 1.1 — Human user identification and authentication	Every human user authenticated through your upstream identity provider before reaching any system inside the OT zone. No shared accounts. Every session is tied to a verified identity. Service accounts and AI agents identified under the same framework.
SR 1.2 — Software process and device identification	Non-human identities (service accounts, software processes, AI agents, devices) authenticated through certificates, OAuth, OIDC, or service mesh identity systems before reaching OT-adjacent systems.
SR 1.5 — Authenticator management	TAC consumes authenticators from the upstream IdP; lifecycle management remains in your identity source of truth. TAC can issue session-scoped tokens with no portability outside the proxy.
SR 1.7 — Strength of password-based authentication	MFA enforced on every session regardless of upstream password strength. Multiple factor options including FIDO2 / WebAuthn (phishing-resistant), hardware tokens, push, OTP, SMS, TOTP, and third-party providers.
SR 2.1 — Authorisation enforcement	Per-user, per-system, per-protocol policy decisions enforced at the proxy on every request. Authorisation is not just an initial check but is continuously evaluated throughout the session; mid-session changes take effect immediately.
SR 2.4 — Mobile code	TAC's reverse proxy inspects requests at the application layer and can enforce policy on the content of traffic, not just the source and destination. Custom JavaScript policies available for advanced payload inspection scenarios (power-user feature).

SYSTEM INTEGRITY & TIMELY EVENT RESPONSE

FR 3 & FR 6 — Primary Coverage

REQUIREMENT	HOW TAC DELIVERS
SR 3.1 — Communication integrity	All TAC-brokered sessions encrypted via TLS 1.2 or TLS 1.3 with FIPS 140-2 compliant cryptographic modules, protecting against tampering and eavesdropping on the access path to OT-adjacent systems.
SR 6.1 — Audit log accessibility	Comprehensive audit log accessible through the TAC console and exportable to SIEM via syslog or API. Every authentication, authorisation, and session event is recorded with full attribution: who, what, when, where, which device, which application, and outcome.

REQUIREMENT	HOW TAC DELIVERS
SR 6.2 — Continuous monitoring	Continuous evaluation of identity, posture, and policy throughout every session. Compliance lapses or policy condition changes trigger real-time session revocation. Native real-time monitoring and alerting on access events and platform health.

RESTRICTED DATA FLOW & RESOURCE AVAILABILITY

FR 5 & FR 7 — Supporting Coverage

REQUIREMENT	HOW TAC DELIVERS
SR 5.1 — Network segmentation	TAC enforces the conduit between IT zones and OT zones. The IT/OT DMZ becomes a defined boundary with one inbound port and policy-based access control rather than a flat network. (Note: TAC enforces the access-path conduit; broader network segmentation between OT sub-zones requires complementary network infrastructure.)
SR 5.2 — Zone boundary protection	TAC inspects, authenticates, and authorises every request crossing the IT-to-OT zone boundary. Unauthorised traffic is dropped at the proxy. OT-adjacent applications are never directly addressable from the IT side.
SR 7.6 — Network and security configurations	Network access configuration for OT-adjacent systems is centralised in the TAC policy engine, simplifying change management and configuration review. Configuration changes are logged.

> **IEC 62443 Out of Scope: FR 4 — Data Confidentiality (at rest).** FR 4 addresses data confidentiality at rest within OT systems — including encryption of stored process data, configuration files, and historical records. This is a function of the OT applications and storage themselves, not of the access control layer. TAC protects data in transit on the access path but does not address data confidentiality on OT systems directly.

One Platform. Two Frameworks. Same Evidence.

NERC CIP and IEC 62443 use different vocabulary and apply to different industries, but the technical evidence they require for access control, authentication, and monitoring is largely the same. A registered entity preparing for a NERC CIP audit and a manufacturer pursuing IEC 62443 certification are looking at the same questions: who reached which systems, with what authentication, under what policy, and what was logged.

TAC produces this evidence as a natural byproduct of operation. The same audit log that demonstrates CIP-005 ESP enforcement also demonstrates IEC 62443 SR 5.2 zone boundary protection. The same authentication records that satisfy CIP-007 R5 also satisfy IEC 62443 SR 1.1. The same revocation timeline that satisfies CIP-004 R5 also supports IEC 62443 lifecycle requirements.

For organisations preparing for either audit — or both — this matters operationally. You aren't running two separate compliance programmes for OT access. You're running one.

Why TAC for OT Environments

IT/OT DMZ Boundary, Not OT Devices. TAC sits at the IT/OT boundary as a reverse proxy. It enforces who and what can reach the systems that command OT — HMIs, SCADA servers, engineering workstations, historians — without touching the OT devices themselves. PLCs, RTUs, IEDs, and control system components remain entirely unchanged. No agents to deploy on OT systems. No code changes. No certifications to invalidate.

Vendor and Contractor Access — Time-Bounded and Logged. Vendor remote access is one of the most heavily scrutinised areas in both NERC CIP-005 R3 and IEC 62443. TAC scopes vendor sessions to specific systems, enforces MFA on every connection, time-bounds access windows, and logs every action with full attribution. Disabling vendor access is immediate and complete. No orphaned credentials. No shared accounts.

Intermediate System Built In — No Separate Jump Server. NERC CIP-005 R2 requires an Intermediate System for interactive remote access into the ESP. TAC's reverse proxy fulfils this role natively — the proxy IS the Intermediate System. No separate jump server to deploy, harden, monitor, or audit. One platform delivers the boundary control, MFA, and audit trail required.

One Audit Trail, Two Frameworks. The same TAC audit log demonstrates compliance with both NERC CIP and IEC 62443 evidence requirements. Authentication records, authorisation decisions, session timing, and revocation events are captured in one format, exportable to your SIEM. Auditors reviewing different frameworks see the same complete record.

Single Encrypted Port — Conduit Discipline. Both frameworks expect minimum-exposure design at the boundary. TAC closes all inbound firewall ports except one encrypted channel (TLS 1.2 or TLS 1.3 with FIPS 140-2 compliant cryptographic modules) for the OT-adjacent systems it fronts. The IT/OT conduit becomes architecturally tight rather than the typical sprawl of vendor-specific remote-access tools.

OT Compliance Coverage Summary

CONTROL FAMILY / FRAMEWORK	CONTROLS ADDRESSED	TAC COVERAGE
NERC CIP-005	Electronic Security Perimeter	ESP boundary at IT/OT DMZ, Intermediate System for remote access, MFA, vendor access control
NERC CIP-007	System Security Management	Port reduction at ESP boundary, security event monitoring, access control, authentication failure response
NERC CIP-004	Personnel & Access Management	Access management enforcement and same-day revocation evidence (supporting role)
IEC 62443 FR 1 & FR 2	Identification, Authentication, Use Control	Human and non-human identity, MFA, authorisation enforcement, authenticator management
IEC 62443 FR 3 & FR 6	System Integrity, Timely Event Response	TLS 1.2/1.3 with FIPS 140-2 integrity, audit log accessibility, continuous monitoring
IEC 62443 FR 5 & FR 7	Restricted Data Flow, Resource Availability	IT/OT zone conduit, zone boundary protection, centralised network access configuration

Next Steps

Map your OT-adjacent system inventory. Identify every HMI, SCADA server, engineering workstation, historian, and remote-access tool that commands or queries your OT environment. Each is a candidate for TAC mediation. **Request a NERC CIP or IEC 62443 walkthrough** at portsys.com/contact or info@portsys.com — a PortSys specialist will work through your specific OT access architecture and produce a prioritised deployment plan with timeline and milestones.