EPRI

2026 White Paper

ZT4OT Zero Trust for Operational Technology

A Novel High-Assurance Framework for Energy Delivery Systems

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Utilities face mounting pressure from a convergence of forces: evolving threat actors, the emergence of AI-enabled cyber operations that compress the window between disclosure and weaponization, and regulatory drivers such as NERC CIP-015-1[1]. Increasingly, adversaries operate from within authenticated sessions, where traditional identity, perimeter, and network-based controls have limited visibility into whether the activity itself is legitimate. This is where enterprise Zero Trust approaches fall short when applied directly to Operational Technology (OT): they can validate access to the system, but they often lack the engineering and operational context needed to judge whether behavior inside the session should be trusted.

Zero Trust Architecture (ZTA) has become the dominant paradigm for enterprise IT security, driven by NIST SP 800-207 and mandated across federal agencies following the 2021 Executive Order on Improving the Nation's Cybersecurity[2]. Its core principle of "never trust, always verify" is sound, and the threat it now confronts is no longer hypothetical. Anthropic's disclosure of the GTG-1002 campaign[3], in which an AI agent autonomously executed espionage operations against thirty global targets, is a concrete instance of this authenticated-session problem: the adversary operated inside valid sessions without tripping any identity- or network-based control. Applied without modification to OT environments, ZTA leaves fundamental gaps that can undermine both security fidelity and operational safety.

This document articulates a novel framework, EPRI's ZT4OT (Zero Trust for Operational Technology)[4], that extends Zero Trust principles into OT. EPRI's ZT4OT introduces three constructs not commonly defined in current Zero Trust literature or implementation guidance: **System Behavior Analytics** (SBA), a design-derived behavioral baseline for devices and system components; OT-tuned **User and Entity Behavior Analytics** (OT-UEBA) adapted to operational workflows; and the **Context-Aware Trust Controller** (CATC), an OT-specific Policy Decision Point that arbitrates trust decisions across identity, design compliance, device state, and operational context.

[1] https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-015-1.pdf
[2] https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity
[3] https://assets.anthropic.com/m/ec212e6566a0d47/original/Disrupting-the-first-reported-AI-orchestrated-cyber-espionage-campaign.pdf
[4] https://www.epri.com/portfolio/products/000000003002031083

Critically, EPRI's ZT4OT is designed for incremental adoption. A passive deployment mode supports NERC CIP-015 Internal Network Security Monitoring (INSM) compliance with zero operational risk, establishing the behavioral baseline and conformance evidence utilities need today. As confidence in the baseline matures, the framework advances through advisory and active enforcement phases with each transition governed by a risk-based readiness threshold calibrated to asset criticality and operational consequence.

Core Thesis: In OT environments, trust decisions must be derived from system design and operational context, not just identity and network posture. This is the fundamental gap between Enterprise ZT and ZT4OT. Trust requires understanding: EPRI's ZT4OT makes OT systems legible - a prerequisite for meaningful, defensible trust decisions.

1. THE PROBLEM: ENTERPRISE ZERO TRUST APPLIED TO OT

The OT cybersecurity community has invested significantly in adopting enterprise security frameworks. Firewalls, network segmentation, multi-factor authentication, privileged access management, and VPN jump servers are now common in utility environments. These are necessary controls. They are not sufficient for today's advanced threats.

Enterprise Zero Trust products and frameworks were designed for environments characterized by dynamic users, cloud workloads, distributed endpoints, and identity-centric access. OT environments have fundamentally different properties. The prior NERC "Zero Trust for Electric OT"[5] whitepaper identifies four foundational ZT pillars for OT - identity, devices, network/environment, and applications/workloads, and acknowledges that applying these in OT requires significant adaptation. EPRI's ZT4OT extends that foundation by addressing what those pillars cannot reach: the design-derived behavioral layer that makes OT environments fundamentally different from enterprise IT.

Table 1: *Enterprise IT vs. OT: Fundamental Differences.*

Dimension	Enterprise IT	OT / Energy Delivery
Asset Behavior	Dynamic, user-driven activity	Deterministic, design-constrained
Communication Model	Any-to-any with policy controls	Defined topology; expected peers
Client/Server Ratio	Many clients to few servers; user-centric	Few clients (SCADA master) to many servers (RTUs, gateways, relays); M2M-dominated
Identity Model	Human users, cloud identities	Devices, services, engineering roles
Threat Profile	Credential theft, malware, exfiltration	Operational disruption, manipulation
Failure Consequence	Data breach, service outage	Safety failure, grid disruption
Regulatory Context	FISMA, SOC2, HIPAA	NERC CIP, IEC 62443, NIST CSF
Protocol Stack	TCP/IP, HTTP, modern APIs	DNP3, IEC-61850, Modbus, ICCP, IEEE 2030.5

The client/server ratio inversion is particularly significant. Enterprise ZT assumes a large population of users accessing a relatively small set of resources in an identity-centric model where the access request originates with a human. OT environments invert this: a small number of SCADA masters and engineering workstations access a large population of "servers": RTUs, gateways, protection relays, and PLCs. Most traffic is machine-to-machine, with no human in the loop. Enterprise ZT frameworks were not

[5] https://www.nerc.com/globalassets/our-work/reports/white-papers/white_paper_zero_trust_for_electric_ot.pdf

designed for this topology and applying them without modification can produce both gaps and false positive rates that utilities find operationally untenable.

1.1 What Enterprise ZT Gets Right (But Is Not Enough)

Enterprise ZTA delivers meaningful value in OT when applied correctly. The following principles translate well:

- Strong identity verification for engineering access sessions
- Network micro-segmentation between OT zones and IT/DMZ
- Least-privilege access for human operators and vendor accounts
- Continuous session monitoring and logging for compliance

These represent common cyber-hygiene. They address the perimeter and identity layers. They do not address what happens inside a correctly-authenticated and correctly-authorized session in which adversarial or anomalous activity is occurring.

1.2 The Four Critical Gaps

Translating Enterprise ZT into OT without modification creates four structural gaps:

Table 2: *Four Critical Gaps in Enterprise ZT for OT*

Gap	Description	Operational Consequence
1. No System Design Awareness	Enterprise ZT policies are written around identities and resources. OT environments have an additional dimension: the system is architecturally defined and formally documented. This design-derived behavioral model is not provided by current Enterprise ZT products.	Cannot distinguish authorized lateral movement from adversarial lateral movement using valid credentials.
2. No Operational Workflow Context	In OT, the legitimacy of an action depends on when it occurs relative to operational state. Engineering activity during a maintenance window is expected; the same activity at off-hours (e.g., 02:17 am) during steady state is anomalous. Enterprise ZT has no concept of operational workflow state.	Off-hours and out-of-window activity is invisible as a trust signal.
3. No System Behavioral Model	Enterprise UEBA models users and entities, but behavioral expectations are identity- and network-centric not design-derived. In OT, device behavior is architecturally constrained by engineering role and system design. Enterprise UEBA products do not derive behavioral baselines from engineering artifacts or enforce design-specified behavioral envelopes. In addition , enterprise tools are not designed to model the holistic system - the designed interactions between devices and the system-wide process flows that SBA intends to capture.	Device impersonation, protocol misuse, and unauthorized command sequences are invisible. Cross-device interaction anomalies are invisible.

Gap	Description	Operational Consequence
4. Binary Trust Decisions	Enterprise ZT enforcement is fundamentally binary: allow or deny. OT requires nuanced trust responses calibrated to operational risk - graduated responses including step-up verification, command-level validation, operator escalation, or constrained monitoring.	Anomalies during a session cannot be managed with a binary gate without unacceptable operational risk.

The central failure of applying Enterprise ZT to OT: it secures the gate but has no model of what should happen inside the fence. Without that model, you cannot build meaningful trust because trust requires the ability to explain and predict behavior.

2. TERMINOLOGY: CONSTRUCTS INTRODUCED IN THIS WORK

Three terms used throughout this brief are introduced as defined constructs of the EPRI's ZT4OT framework. These constructs are not commonly defined, in the form presented here, in current Zero Trust or behavioral analytics literature. They are presented here so that subsequent sections can reference them without ambiguity.

System Behavior Analytics (SBA)

An analytical construct introduced in this work. SBA models the expected holistic behavior of the OT environment as an integrated system - the designed interactions between devices, the topology of communications, the sequencing of process-level operations, and the cross-system data flows defined by engineering documentation. Where UEBA models the expected behavior of individual entities (users and devices), SBA models the system as a whole, enabling detection of violations invisible at the entity level: interactions between devices that are individually valid but collectively violate the designed system behavior.

OT-Tuned User and Entity Behavior Analytics (OT-UEBA)

An adaptation of standard UEBA - User and Entity Behavior Analytics introduced in this work as a defined construct for OT operational workflows. Standard UEBA models users and non-human entities through observed behavioral patterns. OT-UEBA extends this with two OT-specific dimensions: (1) operational workflow state as a trust signal, and (2) device engineering roles as the context for expected entity behavior. OT-UEBA operates at the entity level while SBA operates at the system level.

Context-Aware Trust Controller (CATC)

A trust decision construct introduced in this work. CATC is an OT-specific instantiation of the NIST SP 800-207 Policy Decision Point (PDP). Outputs are graduated rather than binary: allow, step-up authentication, command-level validation, escalation, observe-only, or active isolation, calibrated to operational consequence.

Asset Graph

A multi-layer machine-readable representation of the OT environment derived from engineering artifacts (one-line diagrams, relay configuration files, asset inventories, protocol role assignments, and operational workflow documentation). The Asset Graph encodes physical connectivity, protocol relationships, logical data flows, and engineering access patterns as distinct analytical layers. It serves as the formal behavioral specification at both the system level (for SBA) and the entity level (for OT-UEBA) against which observed activity is evaluated.

3. EPRI'S ZT4OT FRAMEWORK: ARCHITECTURE AND COMPONENTS

EPRI's ZT4OT addresses the four gaps identified in Section 1 by adding three layers to the foundational Enterprise ZT controls: System Behavior Analytics (SBA), operationally-tuned UEBA (OT-UEBA), and the Context-Aware Trust Controller (CATC). Together, these transform identity- and network-centric Zero Trust into a design-aware, operationally-contextual enforcement architecture.

The framework is organized as a layered decision stack:

Table 3: *ZT4OT Five-Layer Decision Stack.*

LAYER 1 - Engineering Design Model Asset Inventory | Communication Topology | Device Roles | Protocol Bindings | Utility Process Documentation
LAYER 2 - Identity & Role Graph Engineering Identities | Access Rights | Role Assignments | Credential Posture
LAYER 3 - Telemetry & Monitoring Network Flows | Protocol Messages | Device Logs | Engineering Session Data | Operational Readings (V/I/F)
LAYER 4 - Behavioral Analytics Engine System Behavior Analytics (SBA) | OT-Tuned UEBA | Anomaly Correlation | RNN/GNN Temporal + Graph Analysis
LAYER 5 - Context-Aware Trust Controller (CATC) Operational Context | Risk Scoring | Policy Engine | Trust Decision | Phase Governance
OUTPUTS - Enforcement Actions Passive Alert | Advisory Recommendation | Step-Up Auth | Command Validate | Escalate | Observe-Only | Active Isolation

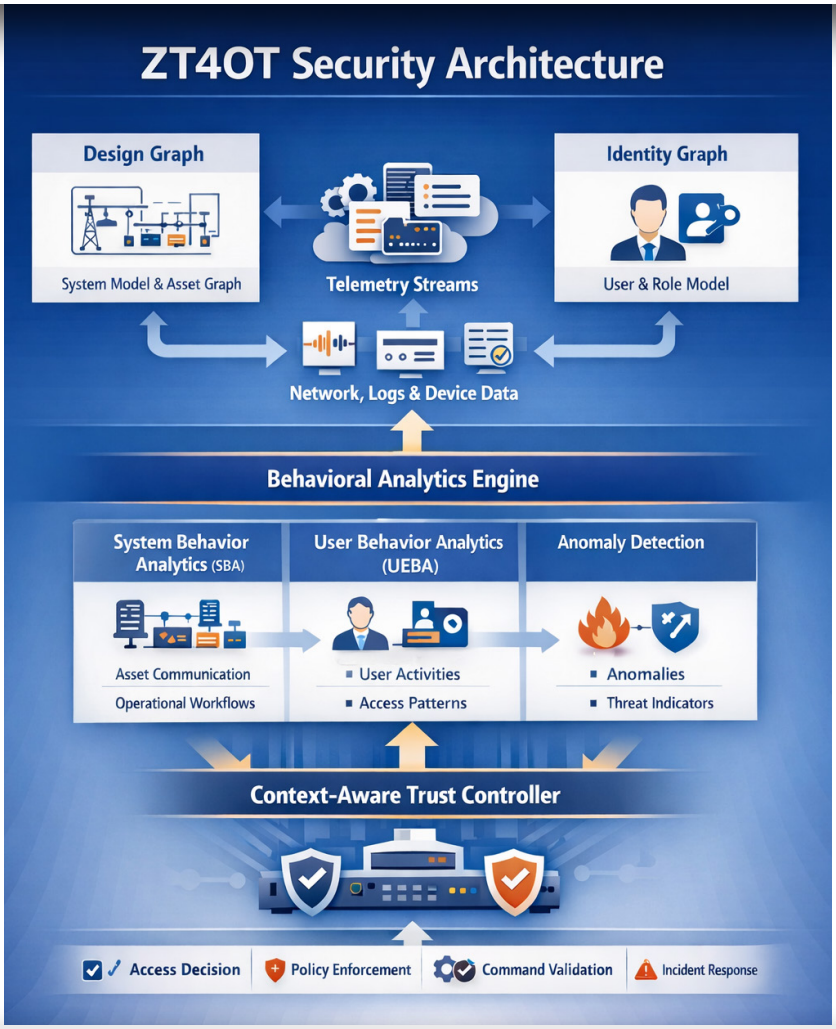

Figure 1: *EPRI's ZT4OT Security Architecture showing Design Graph, Identity Graph, Telemetry Streams, Behavioral Analytics Engine, and Context-Aware Trust Controller.*

3.1 Layer 1 — Engineering Design Model

The foundation of EPRI's ZT4OT is a machine-readable representation of the infrastructure derived from engineering artifacts. This model answers: what is this system designed to do, and how is it expected to behave? It is the key differentiator between EPRI's ZT4OT and current ZT products - it encodes what the system is supposed to do before any telemetry is observed.

Inputs to the Design Model include:

- Substation one-line and communication diagrams
- Protection relay and RTU configuration files
- Network architecture and firewall rule sets
- Asset inventories (IP addresses, MAC addresses, device types, firmware versions)
- Protocol role assignments (DNP3 master/outstation, IEC-61850 publisher/subscriber, Modbus master/slave)
- Utility process documentation: maintenance schedules, change management records, operating procedures defining expected timing and sequencing of engineering activities

The Design Model produces a multi-layer Asset Graph capturing device roles and relationships across distinct analytical layers:

- Physical connectivity layer: which devices are physically interconnected via copper, fiber, or serial
- Protocol layer: which devices communicate at the application layer and in what role
- Logical data flow layer: which data objects move between which systems and in which direction
- Engineering access layer: which human roles access which devices under which conditions

This multi-layer structure allows EPRI's ZT4OT to detect anomalies that span layers, for example a device physically connected and communicating at the protocol layer but whose data flows violate the logical design, or an engineering session that is identity-valid but occurs outside expected access layer context.

A key insight motivates this design: if enterprise IT environments were documented to the same standard as OT - with one-line diagrams, communication matrices, device configuration files, and protocol role assignments then enterprise ZT frameworks could leverage that documentation in the same way EPRI's ZT4OT does. OT's engineering documentation culture, often seen as a legacy burden, is a security asset. EPRI's ZT4OT operationalizes that data.

Research Challenge: How do we reliably convert heterogeneous engineering artifacts - Visio diagrams, relay configuration files, vendor-specific formats, utility procedure documents - into a standardized, machine-readable multi-layer Asset Graph? What level of human validation is required, and can the process be automated across different utility environments?

3.2 Layer 2 — Identity & Role Graph

The Identity & Role Graph captures the human and machine identity layer of the OT environment. It provides the context against which engineering access sessions are evaluated by the CATC. Components include:

- Engineering identities: authenticated user accounts with role assignments (protection engineer, operations engineer, vendor, administrator)
- Access rights: which identities are authorized to access which devices, under which conditions, and via which access paths
- Role assignments: the operational role of each identity relative to specific substations, assets, or maintenance activities
- Credential posture: MFA enrollment status, credential age, session history, and anomaly history

The Identity Graph is a standard ZT construct. Within ZT4OT it serves as one of five trust signal inputs to the CATC, it is necessary but not sufficient for a trust decision. A valid identity with a clean credential posture does not authorize behavior that violates the Design Model or falls outside the operational workflow baseline.

***Table 4**: SBA Detection Capability vs. Traditional SIEM/IOC*

Detection Type	Traditional SIEM / IOC	SBA (ZT4OT)
Basis for Detection	Known bad IPs, hashes, signatures	Design-derived behavioral baseline
Novel Attacks	Blind	Detected (baseline violation)
Valid Credentials Used	Blind	Detected (anomalous behavior)
Cross-Device Anomaly	Blind (no system model)	Detected (system-level topology violation
Protocol Misuse	Rule-dependent	Detected (unexpected protocol)
Insider Threat	Poor	Strong (workflow awareness)
Alert Context	Alert + threat intel lookup	Device role + topology + action + operational state

3.3 Layer 3 — Telemetry & Monitoring

The Telemetry layer provides the observed activity stream against which the Asset Graph behavioral specification is evaluated. It is passively collected with zero operational impact via network TAP or SPAN port and includes:

- Network flows: source/destination IP, port, protocol, session duration, byte counts
- Protocol messages: decoded OT protocol communications (DNP3 function codes, IEC-61850 GOOSE/MMS, Modbus register reads/writes)
- Device logs: engineering workstation session logs, jump host access records, device event logs
- Engineering session data: commands issued, configuration changes, access timing, access path
- Operational readings: voltage, current, frequency, breaker state - used as operational context signals for the CATC

Telemetry is the evidentiary input to both SBA (system-level behavioral evaluation) and OT-UEBA (entity-level behavioral evaluation). Raw telemetry has no trust signal context in isolation; its significance is determined by comparison to the Asset Graph behavioral specification.

3.4 Layer 4a — System Behavior Analytics (SBA)

We introduce **System Behavior Analytics (SBA)** as a new analytical construct: the holistic system-level counterpart to entity-level UEBA. Where UEBA models expected human behavior from observed activity, SBA models expected behavior of the OT environment as an integrated system derived directly from engineering design. SBA is concerned with how the system as a whole is designed to function, not how any individual device or user is expected to behave in isolation.

SBA as defined here by holistic system scope rather than entity scope, design-derived rather than statistically baselined alone, and integrated with a ZT enforcement architecture is not, in this integrated form, formally defined in current OT Zero Trust architectures. Specification-based intrusion detection for ICS is an established research area (Cheung, Carcano, and others); SBA advances those works by formalizing design-derived behavioral specifications at the system level and integrating them into a graduated ZT enforcement architecture through the CATC.

Critically, SBA detects anomalies invisible to any entity-level tool: two devices each behaving normally in isolation, but whose interaction violates the designed system topology or process flow.

Table 5: *CATC Trust Decision Matrix*

Decision	Trigger Condition	Enforcement Action
Allow	All context signals within baseline	Session permitted with logging
Step-Up Auth	Elevated risk score, off-hours, unfamiliar workstation	Require additional verification (push/call/supervisor approval)
Command Validate	Session allowed; specific command triggers anomaly signal	Require operator confirmation per command
Escalate	Multiple correlated anomalies across SBA and OT-UEBA	Alert SOC analyst for review; optionally restrict
Observe-Only	Session anomalous but operational disruption risk is high	Session continues with elevated monitoring and recording no automated blocking. Safety-critical systems maintain this mode permanently regardless of anomaly score.

ZT4OT intentionally challenges two deeply held assumptions in OT security: that behavioral baselining must be learned statistically, and that enforcement must be binary or absent. We expect informed disagreement on both points.

3.5 Layer 4b — Operationally-Tuned UEBA

EPRI's ZT4OT incorporates UEBA principles adapted for OT operational workflows.

Standard UEBA - User and Entity Behavior Analytics already models both human users and non-human entities. OT-UEBA adds two dimensions absent from enterprise implementations: operational workflow state and device engineering roles as determinants of expected entity behavior. OT-UEBA operates at the entity level; SBA (Section 3.4) operates at the system level. They are complementary.

OT-UEBA behavioral dimensions considered:

- Identity pattern: Is this the engineer who normally works this substation?
- Device access context: Is this the expected engineering workstation or jump host?
- Operational workflow: Is this access occurring during a scheduled maintenance window consistent with utility process documentation?
- Command pattern: Are the relay commands consistent with the stated maintenance purpose?
- Entity behavioral scope: Does observed device behavior conform to its engineering role?

The power of EPRI's ZT4OT emerges when SBA and OT-UEBA signals are correlated. An engineer logging in outside normal hours is a weak signal. An engineer logging in outside normal hours while the relay initiates an unexpected outbound connection is a stronger combined signal. Neither system alone produces high-confidence detection; together they do.

3.6 Layer 5 — Context-Aware Trust Controller (CATC)

We introduce the **Context-Aware Trust Controller (CATC)** as a novel OT-specific instantiation of the NIST SP 800-207 Policy Decision Point. The CATC differs from existing PDP implementations by ingesting design compliance and operational workflow state as primary trust signals alongside identity and device posture. A comparable construct is not commonly defined in current OT Zero Trust implementation guidance. The CATC replaces the binary allow/deny of enterprise ZT with adaptive trust decisions informed by the full context stack.

A key design principle: trust requires understanding. The CATC can only make defensible trust decisions because the Asset Graph and behavioral baselines make the system legible - expected behavior is formally specified, and deviations are measurable.

Trust decision inputs:

- Identity confidence: authentication strength, credential history, anomaly score
- Device posture: asset role match, configuration state, firmware integrity
- Design compliance: does the requested action conform to the Asset Graph?
- Workflow state: is the operational context consistent with this action per utility process documentation?
- SBA anomaly score: are current system-level behavioral signals within the holistic baseline?
- OT-UEBA anomaly score: are current entity-level behavioral signals within expected bounds?

4. ILLUSTRATIVE SCENARIO: COMPROMISED ENGINEERING CREDENTIAL

4.1 Scenario Setup

Let's explore how SBA, CATC, and OT-UEBA work together in practice by walking through a scenario involving compromised substation engineering credentials and compare how traditional ZT approaches this scenario versus ZT4OT In this scenario, we assume:

- That target is a transmission substation with two 500kV lines and associated protection relays
- Engineering access is performed via a jump server with MFA enforced and role-based access in place
- An attacker has compromised the credentials of a protection engineer via spearphishing
- No malware is deployed; no known-bad IPs are involved

4.2 What Traditional ZT Sees

Because traditional ZT focuses on human identities without utilization of OT-specific context: MFA is passed; credentials are validated; and the session is allowed.

The attacker reaches the relay configuration interface. Because traditional ZT has no contextual model to further enforce access in reaction to additional signals, protection settings can be modified. The event may not be detected until an operational failure occurs.

4.3 What EPRI's ZT4OT Sees

EPRI's ZT4OT utilizes multiple points of observation to craft appropriate responses to this same scenario:

Table 6: *Illustrative Scenario: ZT4OT Detection Response.*

Layer	Signal Observed	EPRI's ZT4OT Response
OT-UEBA	Engineer login at 0217 - 4 standard deviations from baseline access time	Soft anomaly flag; step-up auth triggered
OT-UEBA	Workstation is not the engineer's normal device; VPN path is unusual	Anomaly score elevated
SBA	Relay initiates outbound HTTPS connection to unfamiliar IP after engineer session begins	System-level design violation - relay should not initiate outbound traffic per Asset Graph topology. Distinct from NDR: ZT4OT flags this as a design violation with full system context, correlated with the simultaneous OT-UEBA anomaly.
CATC	Combined SBA + OT-UEBA anomaly score exceeds threshold; no scheduled maintenance in workflow context.	Session flagged; SOC escalation; command validation mode activated
CATC	Configuration write command issued to protection setting	Operator approval required; action logged with full context

Result: The attack is detected through behavioral correlation, not because any indicator was known, but because the combination of user behavior, device behavior, and operational context violated the design-derived baseline. The attacker is using valid credentials but cannot hide from ZT4OT.

5. PASSIVE-TO-ACTIVE DEPLOYMENT MODEL

A consistent barrier to Zero Trust adoption in OT is the perceived operational risk of enforcement. Protection engineers are justifiably cautious about any system that could block a legitimate session, delay a protection configuration update, or trigger an unintended isolation event during a generation emergency. EPRI's ZT4OT addresses this directly through a phased passive-to-active deployment model, where each phase transition is governed by a risk-based readiness threshold rather than a calendar.

The model recognizes a fundamental truth about OT security adoption: trust in a security system, like trust in the operational system it monitors, must be earned through demonstrated understanding. The CATC earns operational trust by first proving the fidelity of its behavioral baseline in passive mode before it is permitted to take any enforcement action.

5.1 Phase Model Overview

Table 7: *Phase 1: Passive Detection (CIP-015 Conformance Mode)*

Phase 1: Passive Detection (CIP-015 Conformance Mode)
Trigger: Immediate - no readiness threshold required **CATC Mode: Observe and Alert only - no enforcement actions**
• Passive network TAP or SPAN port captures all internal ESP traffic • Asset Graph built from engineering documentation and telemetry • SBA and OT-UEBA baselines established over 90–360-day learning period • Anomaly alerts generated and routed to SIEM/SOC for analyst review • All anomalies logged with full context for CIP-015 audit evidence • Zero impact on OT operations - CATC is entirely out-of-band • Substation edge + dashboard at ISOC

Baseline learning period variance: The range reflects potential real-world variance in OT environment complexity. Small substations may achieve baseline maturity in 90 days. Large transmission substations with seasonal maintenance cycles, multiple engineering teams, and complex protection schemes may require the full 360 days to capture seasonal workflow patterns. Asset Graph coverage of >90% of devices is the primary maturity indicator, not elapsed time.

Phase 1 delivers immediate CIP-015 INSM conformance value with zero operational risk. The utility gains a formally specified behavioral baseline, design-aware anomaly detection, and an audit-ready evidence trail. This phase can be sustained indefinitely and does not require advancement to Phase 2.

Phase 1 readiness threshold for advancement: sustained false positive rate below 5% on high-confidence alerts over a 60-day operational period, with SOC analyst validation of detection quality.

Table 8: Phase 2: Advisory Mode (Operator-in-the-Loop)

Phase 2: Advisory Mode (Operator-in-the-Loop)
Trigger: Phase 1 readiness threshold met; SOC and protection engineering sign-off **CATC Mode: Recommend - CATC advises; human decides**
• High-confidence anomaly detections generate advisory recommendations to SOC and engineering • Step-up authentication requests sent to engineers; human approves or denies • Command-level validation alerts presented to control room operators for confirmation • No automated enforcement - all actions require explicit human authorization • CATC decision rationale logged alongside human decision for feedback loop • False positive feedback from operators used to refine anomaly scoring model • Builds operational confidence in CATC decision quality before any automation

Phase 2 introduces the CATC into the operational workflow without removing human judgment. This phase is critical for building trust in both directions: the SOC and protection engineers learn to trust CATC recommendations; the CATC model is refined by operator feedback. Most utilities will find that Phase 2 already exceeds their current detection and response capabilities significantly.

Phase 2 readiness threshold for advancement: operator override rate below 1% on step-up auth recommendations (indicating false positive trust decisions), positive utility stakeholder assessment, and formal risk acceptance documented by asset owner.

*Table 9: **Phase 3: Active Enforcement (Risk-Tiered Automation).***

Phase 3: Active Enforcement (Risk-Tiered Automation)
Trigger: Phase 2 readiness threshold met; formal risk acceptance by asset owner **CATC Mode: Enforce - CATC acts autonomously within defined risk tiers**
• Low-risk enforcement actions automated: step-up auth for off-hours access, session recording escalation • Medium-risk enforcement requires human-in-the-loop: command blocking, session restriction • High-risk enforcement (isolation, communications cutoff) requires dual authorization: CATC + SOC analyst • Safety-critical and reliability-impacting systems maintain permanent Observe-Only mode or Phase 2 advisory regardless of anomaly score • Enforcement actions are reversible and logged with full audit trail • Automatic rollback to Phase 2 advisory if false positive rate exceeds threshold • Fleet-level policy propagation via CATC to heterogeneous assets (firewall, switch ACLs, jump server policies)

Phase 3 does not mean full automation. Risk tiering ensures that the most consequential enforcement actions - those that could affect generation, transmission operations, or protection function - always retain human authorization. The CATC automates the decisions where automation is safe; it escalates the decisions where human judgment is required.

5.2 Risk-Based Phase Transition Framework

Phase transitions are governed by three criteria:

Table 10: *Risk-Based Phase Transition Framework*

Criterion	Phase 1 → 2	Phase 2 → 3	Auto-Rollback Trigger
Detection Quality	FP rate <5% on high-confidence alerts over 60 days	Override rate <1% on advisory recommendations	FP rate exceeds 2% in 30-day window
Baseline Maturity	Asset Graph covering >90% of ESP devices	Seasonal workflow patterns captured (planned/unplanned events)	Significant topology change without model update
Stakeholder Readiness	SOC and engineering review of alert quality	Formal risk acceptance by asset owner; ISOC integration	Engineering escalation due to operational impact

The passive-to-active model resolves the central tension in OT security adoption: protection engineers need confidence that a security system will not cause the failure it is trying to prevent. By making the baseline legible, the detection transparent, and the enforcement graduated - EPRI's ZT4OT earns operational trust the same way all trust is earned in critical infrastructure: through demonstrated competence under observation, before authority is granted.

6. NERC CIP-015 (INSM) ALIGNMENT

NERC CIP-015 - Internal Network Security Monitoring - requires applicable BES Cyber Systems to implement monitoring of internal network communications within the Electronic Security Perimeter. CIP-015 is the regulatory driver that most directly exposes the limitations of existing signature-based and enterprise-adapted security tools.

6.1 Capability Mapping

Table 11: *NERC CIP-015 Capability Mapping*

CIP-015 Objective	Current Tools (Gap)	EPRI's ZT4OT Response
Monitor internal network communications	Passive flow capture with limited analysis context	SBA provides design-aware communication analysis
Detect anomalous lateral movement	Signature-dependent; valid credential blind	Asset Graph detects topology violations regardless of credential
Identify unauthorized engineering access	Login logging; no workflow context	OT-UEBA detects access outside operational workflow baseline
Detect abnormal command execution	Rule-based triggers; high false positive rate	CATC command validation against design-derived expectations
Evidence of normal baseline	Difficult to articulate formally	Asset Graph + SBA baseline provide formal behavioral specification

6.2 Potential Conformance Posture by Deployment Phase

***Table 12**: CIP-015 Potential Conformance Posture by Deployment Phase*

Phase 1 - Passive	Phase 2 - Advisory	Phase 3 - Active
CIP-015 INSM alignment	CIP-015 + enhanced incident response	CIP-015 + ZT enforcement + automated response
Behavioral baseline established	Baseline validated by operator feedback	Baseline drives automated policy
Audit-ready evidence trail	Human decision log + CATC rationale	Full enforcement audit trail
Zero operational risk	Low operational risk; human in loop	Risk-tiered; safety systems excluded

Key regulatory value: For CIP-015 "How do you know what normal looks like inside your ESP?" EPRI's ZT4OT provides a technically credible, architecture-grounded answer. The Asset Graph is the formal behavioral specification; deviations are measurable and auditable.

7. PRIOR WORK AND STRATEGIC POSITIONING

EPRI's ZT4OT builds on a growing body of Zero Trust research and federal guidance while addressing architectural and analytical gaps that remain unresolved. This section situates the framework against four anchors: NIST canonical ZTA, federal OT-specific guidance, academic prior art, and strategic lineage from industry.

7.1 Canonical Alignment with NIST SP 800-207

EPRI's ZT4OT is architecturally aligned with NIST SP 800-207[6] , which defines Zero Trust Architecture in terms of policy decision points (PDPs), policy enforcement points (PEPs), and continuous evaluation of trust signals. Within this model, the Context-Aware Trust Controller fulfills the role of an OT-specific PDP, synthesizing identity assurance, design compliance, behavioral analytics, and operational context to render trust decisions. Enforcement actions are implemented through distributed OT-appropriate PEPs - jump hosts, secure gateways, firewalls, and engineering access controls.

This alignment ensures that EPRI's ZT4OT extends, rather than replaces, the canonical ZTA model, while addressing trust signals (system design and operational state) that are outside the scope of existing enterprise-centric interpretations of NIST SP 800-207. Practical implementation guidance such as NIST SP 1800-35[7]provides direction for deploying Zero Trust using commercial technologies; EPRI's ZT4OT complements this work by addressing elements that current implementation guides intentionally leave undefined - the derivation of system-level behavioral baselines, the correlation of system and user behavior in OT, and the arbitration of trust decisions where enforcement carries operational and safety implications.

7.2 Complementarity with Federal OT Zero Trust Guidance

Recent federal guidance - including the joint CISA, DoD, DOE, FBI, and DOS publication "Adapting Zero Trust Principles to Operational Technology" (April 2026)[8], and the DoD CIO "Zero Trust for Operational Technology Activities and Outcomes" (November 2025)[9] - provides much-needed direction on how Zero Trust must be adapted to OT constraints. That guidance correctly emphasizes safety, availability, legacy constraints, and the risks of directly applying enterprise IT-centric Zero Trust controls to OT systems.

[6] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
[7] https://csrc.nist.gov/pubs/sp/1800/35/2prd
[8] https://www.cisa.gov/sites/default/files/2026-04/joint-guide-adapting-zero-trust-principles-to-operational-technology_508c.pdf
[9] https://www.dmi-ida.org/download-pdf/pdf/ZT-OperationalTechnologyActivitiesOutcomes.pdf

EPRI's ZT4OT is fully aligned with the principles and cautions outlined in this federal guidance. The scope and intent of EPRI's ZT4OT are distinct and complementary: where federal guidance focuses on what considerations must be accounted for when applying Zero Trust to OT, EPRI's ZT4OT addresses how trust decisions can be formally derived, evaluated, and enforced once those constraints are acknowledged. Three specific extensions are worth noting:

- **Design-derived behavioral trust as a missing architectural element**. Federal guidance highlights the value of baseline-based and specification-based detection but intentionally avoids prescribing mechanisms for deriving operational specifications. EPRI's ZT4OT addresses this gap through SBA, which derives expected device and system behavior directly from how the OT system was engineered to function. The Asset Graph serves as an explicit behavioral specification against which observed activity can be evaluated in real time.
- **Context-aware trust decisions beyond binary enforcement.** Federal guidance stresses that OT controls must avoid disrupting safety-critical operations but stops short of defining an architectural mechanism for nuanced, safety-aware trust decisions under anomalous conditions. The CATC fills this gap by integrating identity assurance, device posture, design compliance, workflow state, and correlated SBA/UEBA signals to produce graduated trust responses calibrated to operational consequence.
- **Passive-to-active adoption as an operational governance model.** Federal guidance emphasizes risk-informed decision-making and phased transitions but does not define a concrete governance model for advancing capabilities over time. EPRI's ZT4OT operationalizes this through the passive-to-active model in Section 5, anchoring early deployment in CIP-015-aligned passive monitoring and tying advancement to measurable readiness thresholds.

7.3 Prior Academic Works

Recent research has explored extending Zero Trust beyond static identity and perimeter controls. Notably, ZenGuard (Scientific Reports, 2025)[10] proposes an architecture integrating Zero Trust with SIEM, SOAR, and User and Entity Behavior Analytics (UEBA) for adaptive trust decisions in enterprise environments. ZenGuard demonstrates the feasibility of coupling behavioral analytics with enforcement logic in a continuous decision loop, advancing Zero Trust from gatekeeping toward runtime authorization.

EPRI's ZT4OT aligns with this trajectory but diverges fundamentally in the object of trust and the source of behavioral expectation. ZenGuard's trust decisions are derived from user-centric and workload-centric behavior in enterprise IT systems. EPRI's ZT4OT operates in OT environments where the primary trust subject is the engineered system and physical process itself, not the human user. Where ZenGuard extends UEBA in IT, EPRI's ZT4OT introduces SBA - a distinct construct - for OT, modeling design-constrained device and system behavior derived directly from engineering artifacts. This shift, from user behavior to system behavior as the dominant trust signal, is essential for OT environments and is not a focus of mainstream enterprise ZTA research.

Earlier academic work on ZT in the energy sector includes Alagappan, Venkatachary & Andrews (Energy Reports, 2022)[11] on augmenting Zero Trust Network Architecture for virtual power plants, which establishes the descriptor space for ZT in DER and distributed generation contexts. EPRI's ZT4OT extends this lineage with a formal design-derived modeling layer rather than a network-architecture overlay.

[10] https://www.researchgate.net/publication/396500051_ZenGuard_a_machine_learning_based_zero_trust_framework_for_context_aware_threat_mitigation_using_SIEM_SOAR_and_UEBA

[11] https://www.researchgate.net/publication/357447163_Augmenting_Zero_Trust_Network_Architecture_to_enhance_security_in_virtual_power_plants

7.4 Strategic Lineage: Industry Perspectives

The adaptive trust philosophy underlying EPRI's ZT4OT is directionally consistent with Gartner's Continuous Adaptive Risk and Trust Assessment (CARTA)[12], which emphasizes continuous risk evaluation and context-aware security decisions rather than static access control. CARTA establishes an important strategic principle: trust must be continuously reassessed as context evolves.

EPRI's ZT4OT acknowledges this lineage while remaining architecturally distinct. CARTA is a strategic framework describing what security programs should aspire to. The CATC is a concrete OT-specific trust control construct that operationalizes adaptive trust decisions in deterministic, safety-critical environments. CATC is not a rebranding or implementation of CARTA, but a purpose-built control plane designed to arbitrate trust decisions where incorrect enforcement may have immediate physical or safety consequences.

Industry thought leadership has increasingly recognized that Zero Trust principles must extend beyond human identity to encompass machines, devices, and autonomous systems. Capgemini's "Machines Need Zero Trust Too" (2025)[13], for example, argues for applying context-aware trust to non-human entities in OT and cyber-physical environments, highlighting the inadequacy of purely identity-centric security models as automation increases. EPRI's ZT4OT advances this direction by formalizing how machine and process trust is computed: rather than treating devices as generic endpoints, EPRI's ZT4OT derives expected behavior from the engineering design and operational role of each asset, moving the concept of "machine trust" from an editorial position to a formal, enforceable security architecture.

7.5 Position in the OT Cybersecurity Landscape

Table 13: *ZT4OT Position in the OT Cybersecurity Landscape.*

Field / Product Category	What It Does Well	EPRI's ZT4OT Differentiator
Enterprise ZTA (NIST 800-207)	Identity, segmentation, device posture	Adds design model, OT workflow context, adaptive enforcement
NERC ZT for OT (2023 whitepaper)	ZT pillar framework for electric OT; policy guidance	Extends with design-derived behavioral model, CATC enforcement, passive-to-active path
OT NDR	Asset discovery, protocol visibility, signature detection	Trust enforcement, design-derived baselines, workflow context
SIEM + SOAR	Log correlation, playbook automation	Behavioral baselines replace rules; design context replaces threat intel lookup
Enterprise UEBA	User behavior modeling, identity analytics	Device/system behavior modeling; operational workflow context
PAM / Jump Servers	Session gating, credential management, recording	Command-level validation; design-aware session monitoring

EPRI's ZT4OT is to OT security what UEBA was to enterprise identity security: a new category defined by a more sophisticated behavioral model tuned to the specific characteristics of the environment. The novelty is not in any single component but in the unified, design-derived trust decision architecture.

[12] https://www.ssh.com/academy/iam/carta

[13] https://www.capgemini.com/us-en/insights/expert-perspectives/machines-need-zero-trust-too-why-devices-deserve-context-aware-security/

8. OPEN RESEARCH QUESTIONS

EPRI's ZT4OT is a research-stage framework with several significant open problems. These represent both the intellectual core of the research program and the areas where research funding is well-justified.

RQ1: Design Model Ingestion. How can heterogeneous engineering artifacts - relay configuration files, protection diagrams, asset inventories, utility process documentation, network documentation - be reliably converted into a standardized, machine-readable multi-layer Asset Graph? What level of human validation is required?

RQ2: Behavioral Expectation Derivation. Can expected device behaviors be automatically derived from a Design Model, or must they be manually specified? How are behavioral baselines maintained as systems evolve through maintenance, upgrades, and reconfiguration?

RQ3: Contextual Anomaly Scoring. How are SBA and UEBA signals combined into a reliable anomaly score without excessive false positives? What weighting model correctly reflects the relative significance of different signal types across different operational contexts?

RQ4: Trust Enforcement in Safety-Critical Environments. What are the appropriate enforcement responses for EPRI's ZT4OT in environments where incorrect denial of access could cause safety failures? How does the CATC balance security response with operational availability requirements? This question is directly addressed by the passive-to-active deployment model in Section 5.

RQ5: Utility Testbed Validation. Can EPRI's ZT4OT be demonstrated in a representative energy delivery environment with sufficient fidelity to evaluate operational impact, detection effectiveness, and false positive rates? EPRI's CSRL combined with proposed POCs provides the primary validation environment for TRL 5-6 demonstration.

9. SUMMARY

EPRI's ZT4OT is not a product, a vendor category, or a checklist. It is a research-backed security architecture that addresses the specific properties of energy delivery environments that Enterprise ZT frameworks were not designed to handle.

Its core innovation is deriving trust decisions from system design: the multi-layer Asset Graph becomes the behavioral specification, and deviations from that specification become the basis for detection and enforcement - regardless of whether credentials are valid, protocols are legitimate, or threat intelligence has a matching indicator.

The three constructs introduced in this work - System Behavior Analytics (SBA), operationally-tuned UEBA (OT-UEBA), and the Context-Aware Trust Controller (CATC), address each of the four structural gaps in Enterprise ZT for OT: absence of design awareness, absence of operational workflow context, absence of device-role behavioral baselines, and inadequacy of binary trust enforcement.

The passive-to-active deployment model resolves the adoption barrier: utilities can deploy EPRI's ZT4OT in passive CIP-015 conformance mode immediately, with zero operational risk, and advance to advisory and active enforcement as the behavioral baseline matures and operational confidence is established.

The framework is timely. CIP-015 INSM requirements are forcing utilities to confront gaps in their current detection

capabilities inside the ESP. ZT approaches are being mandated across federal infrastructure. AI/ML capabilities - particularly GNN-based device relationship modeling and RNN-based temporal anomaly detection - are now mature enough to support the behavioral modeling that EPRI's ZT4OT requires, deployable on edge hardware that fits within substation power and space budgets.

EPRI is uniquely positioned to develop, validate, and publish EPRI's ZT4OT with access to utility partners, the CSRL research testbed, regulatory engagement, and the domain expertise in energy delivery systems that the framework demands.

What utilities can do next: Begin by evaluating how your current Zero Trust and monitoring implementations account for system design, operational workflow context, and authenticated-session behavior. Phase 1 passive deployment delivers CIP-015 INSM conformance value with zero operational risk, it offers a practical, low-commitment entry point.

EPRI members are encouraged to engage with the ZT4OT Interest Group, join Phase 1 passive deployment discussions, and help shape future validation and pilot activities.

For more information, contact Chuck Moran (cmoran@epri.com**), John Stewart (**jstewart@epri.com**) or visit the** ZT4OT Supplemental Project Notice.

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

REFERENCE HEREIN TO ANY SPECIFIC COMMERCIAL PRODUCT, PROCESS, OR SERVICE BY ITS TRADE NAME, TRADEMARK, MANUFACTURER, OR OTHERWISE, DOES NOT NECESSARILY CONSTITUTE OR IMPLY ITS ENDORSEMENT, RECOMMENDATION, OR FAVORING BY EPRI.

EPRI CONTACTS

CHUCK MORAN, *Principal Technical Leader*
650.855.8521, cmoran@epri.com

JOHN STEWART, *Principal Technical Leader*
865.218.8197, jstewart@epri.com

About EPRI

Founded in 1972, EPRI is the world's preeminent independent, nonprofit energy research and development organization, with offices around the world. EPRI's trusted experts collaborate with more than 450 companies in 45 countries, driving innovation to ensure the public has clean, safe, reliable, and affordable access to electricity across the globe. Together...Shaping the Future of Energy.®

AI Use

Your use of this product with AI tools will follow the internal business use terms of the respective agreement between your company and EPRI. You understand that some AI tools do not protect intellectual property and can produce inaccurate or biased results. Furthermore, you understand that use of this product with AI tools in an unauthorized manner may trigger contractual remedies and/or lead to significant consequences.

Export Control Restrictions

Access to and use of this EPRI product is granted with the specific understanding and requirement that responsibility for ensuring full compliance with all applicable U.S. and foreign export laws and regulations is being undertaken by you and your company. This includes an obligation to ensure that any individual receiving access hereunder who is not a U.S. citizen or U.S. permanent resident is permitted access under applicable U.S. and foreign export laws and regulations.

In the event you are uncertain whether you or your company may lawfully obtain access to this EPRI product, you acknowledge that it is your obligation to consult with your company's legal counsel to determine whether this access is lawful. Although EPRI may make available on a case by case basis an informal assessment of the applicable U.S. export classification for specific EPRI products, you and your company acknowledge that this assessment is solely for informational purposes and not for reliance purposes.

Your obligations regarding U.S. export control requirements apply during and after you and your company's engagement with EPRI. To be clear, the obligations continue after your retirement or other departure from your company, and include any knowledge retained after gaining access to EPRI products.

You and your company understand and acknowledge your obligations to make a prompt report to EPRI and the appropriate authorities regarding any access to or use of this EPRI product hereunder that may be in violation of applicable U.S. or foreign export laws or regulations.

For more information, contact:

EPRI Customer Assistance Center
800.313.3774 • askepri@epri.com

June 2026

EPRI
3420 Hillview Avenue, Palo Alto, California 94304-1338 USA • 650.855.2121 • www.epri.com