Zero Trust for Critical Infrastructure: Policy, Architecture, and Implementation Roadmap for the Power Sector

IJIMSR, Vol. 3, No. 1, (2025) 25.3.1.027

***Dr. Jatin Patel**
Associate Professor
(IT) - SITAICS,
Rashtriya Raksha University, Gujarat
Email: jatin.patel@rru.ac.in

***Corresponding author**

Received 18th Nov 2025; Accepted 23rd Dec 2025

KEYWORDS: Power Sector, Cybersecurity, Zero Trust Architecture, Micro Segmentation, Identity Management, and Policy Enforcement

Zero Trust for Critical Infrastructure: Policy, Architecture, and Implementation Roadmap for the Power Sector

Dr. Jatin Patel
Associate Professor
(IT) - SITAICS,
Rashtriya Raksha University, Gujarat
Email: jatin.patel@rru.ac.in

ABSTRACT

Critical infrastructure sectors such as the power grid are increasingly targeted by sophisticated cyberattacks exploiting the convergence of Information Technology (IT) and Operational Technology (OT) networks. Traditional perimeter-based security mechanisms are inadequate to address insider threats, lateral movement, and compromised remote access. This paper proposes a Zero Trust Architecture (ZTA) tailored for the power sector, integrating policy-driven access control, adaptive trust scoring, micro segmentation, and continuous verification across IT–OT environments.

The proposed framework aligns with international standards including NIST SP 800-207 ' and IEC 62443 , and incorporates sector-specific regulatory requirements. A realistic simulation testbed was developed to validate the architecture using representative threat scenarios. Experimental results demonstrate an 83% reduction in unauthorized lateral movement, a 75% decrease in anomaly detection time, and a 90% improvement in mean time to revoke access (MTTRA) compared to traditional security models, while maintaining policy enforcement latency below 5 ms, ensuring operational suitability for real-time power systems.

KEYWORDS: Power Sector, Cybersecurity, Zero Trust Architecture, Micro Segmentation, Identity Management, and Policy Enforcement

ACRONYMS

i. Zero Trust Architecture (ZTA)
ii. Information Technology (IT)
iii. Operational Technology (OT)
iv. Supervisory Control and Data Acquisition (SCADA)
v. Industrial Control Systems (ICS)
vi. Policy Decision Point (PDP)
vii. Policy Enforcement Point (PEP)
viii. Policy Administration Point (PAP)
ix. Identity Provider (IdP)
x. Security Information and Event Management (SIEM)
xi. User and Entity Behavior Analytics (UEBA)
xii. Programmable Logic Controller (PLC)
xiii. Remote Terminal Unit (RTU)
xiv. Intelligent Electronic Device (IED)
xv. Central Electricity Authority (CEA)
xvi. National Critical Information Infrastructure Protection Centre (NCIIPC)
xvii. Cybersecurity Capability Maturity Model (C2M2)
xviii. Multi-Factor Authentication (MFA)
xix. Attribute-Based Access Control (ABAC)
xx. Mean Time to Revoke Access (MTTRA)

1. INTRODUCTION

Sophisticated cyberattacks which designed to target substations, grid management networks, and Supervisory Control and Data Acquisition (SCADA) architectures are becoming more common in the power industry. Conventional boundary based security is unsuccessful against lateral movement, insider threats, and supply chain compromise, as evidenced by incidents like the 2015 Ukraine power grid attack and malware penetration in ICS networks.

Existing OT equipment without authentication, vendor remote access and limited clarity across IT-OT boundaries are some of the main issues. Once access is granted, traditional controls like firewalls, VPNs, and IDS-IPS do not offer continuous monitoring or adaptive trust determinations.

The proposed, a Zero Trust Architecture (ZTA) created dedicatedly for power infrastructure to identify security gaps. Through authentication, device identity, micro segmentation, and policy-based continuous verification, the framework defines the "never trust, always verify" tenets. It also enables dynamic access control, anomaly detection, and stick to cyber security requirements by integrating IT/OT environments under one governance.
While existing studies and standards such as NIST SP 800-207, IEC 62443 ' , and prior research on micro segmentation and industrial cybersecurity provide foundational guidance, they primarily focus on either enterprise IT environments or static defense-in-depth models for OT systems. These approaches do not fully address the operational constraints, legacy device limitations, and continuous trust evaluation required in power sector infrastructures.

In contrast, this paper makes the following contributions:
1.1 Proposes a sector-specific Zero Trust Architecture explicitly tailored for power sector IT–OT environments, integrating operational safety and cybersecurity requirements.

1.2 Introduces a policy-driven, adaptive trust scoring mechanism that dynamically evaluates identity, device posture, behavior, and context.

1.3 Defines a micro segmentation and access enforcement model suitable for legacy SCADA and substation networks without disrupting deterministic control traffic.

1.4 Presents a phased implementation roadmap aligned with regulatory frameworks such as CEA and NCIIPC .
Validates the proposed approach using a realistic simulation testbed and threat scenarios aligned with MITRE ATT & CK for ICS.

2. LITERATURE REVIEW

The limitation of existing perimeter-based cybersecurity models led to the development of the Zero Trust Architecture (ZTA) architecture, which was initially designed by Kindervag (2010) .

ZTA was defined in NIST Special Publication 800-207 ' as a policy enforcement mechanism that regularly check trust before to allowing access. Although its application in Operational Technology (OT) environments especially those regulating critical power infrastructure remains untouched compare to its applicability to enterprise Information Technology (IT) systems is well-established.

ZTA increases resilience for the lateral movement and credential theft in enterprise networks, as Rose et al. showed; nonetheless, OT networks constitute particular difficulties such availability-critical operations, non-IP-based communications, and legacy device limitations ' .

IEC 62443 and ISO/IEC 27019 —— are industrial cybersecurity standards which provide security management and defense-in-depth concepts, but they lack the dynamic policy enforcement and ongoing trust analysis necessary for Zero Trust. Although they acknowledge ZTA as a viable strategy for critical infrastructure(CI), the U.S. Department of Energy's C2M2 Framework and CISA's ICS Zero Trust guidelines do not provide architecture-level integration with current SCADA, DCS, EMS and other systems.

Barriers include protocol incompatibility (e.g., IEC 61850, DNP3, Modbus), limited device attestation support, and difficulties in implementing multi-factor authentication in control networks are mentioned in Gartner's study on Zero Trust in ICS networks [13]. According to N. K. Malhotra et al., full ZTA enforcement is not feasible without safety-aware policy tweaking since OT networks frequently operate under deterministic communication and real-time control limitations [11].

To lessen lateral movement, researchers Lai et al. and T. Alves et al. identified the integration of micro segmentation and anomaly detection within substations [9], [10]. Although these methods show increased detection accuracy, they mostly depend on static trust models that are inappropriate for heterogeneous OT devices and IT-centric orchestration.

An AI-driven adaptive trust mechanism for Industrial IoT that regularly modifies access based on behavioural analytics is proposed in other scholarly publications, such as S. Shrestha et al. [12]. However, these models are not supporting for the regularly work with the human-machine interfaces (HMIs), RTUs, and outdated PLCs that are the core part of power sectors.

In conclusion, the literature survey has shown that Zero Trust principles has given some advance security posture in industrial settings; still, there are major challenges to their application.

2.1 Dependencies of Equipment: Majority ICS and SCADA devices lack authentication or encryption mechanism.

2.2 Protocols: Standards like DNP3 and Modbus are lacking in the native Zero Trust hooks.

2.3 Operational challenges: Regular verification can disrupt deterministic control loops.

2.4 Limited Governance: Disjoint IT and OT access policies hamper the centralized policy enforcement in the overall architecture.

2.5 Lack of Adaptive Risk Scoring: Most current models using static policies which is not preferable for the dynamic operational contexts.

To overcome the aforementioned challenges, this paper proposes a robust architecture for a sector-specific Zero Trust Architecture (ZTA) for the power sector integrating:

- Identity-driven access control,
- Device identify and micro segmentation, and
- Adaptive risk-based trust scoring in a unified governance framework.

This approach aligns with various standards like NIST SP 800-207, IEC 62443, and CISA Zero Trust for ICS, while addressing real-world deployment constraints in OT networks.

3. ZERO TRUST POLICY AND FRAMEWORK FOR THE POWER SECTOR

The implementation of ZTA for the power sector needs to align with the national cyber security frameworks, regulations and other international standards for the ICS, SCADA and OT architecture. With reference to other IT and OT architecture, Power sector architectures needs to maintain 99.99% availability and without disturbance in the operational integrity, which requires balanced mechanism for the security and safety assurance.

3.1 Existing Policy and Regulatory Landscape

Globally, there are several frameworks which have mentioned guidance for Zero Trust adoption within industrial or energy infrastructures:

3.1.1 NIST SP 800-207 (Zero Trust Architecture, 2020) ' initiates the conceptual model for policy decision and enforcement points (PDP/PEP), continues authentication, and dynamic access control. Still, it does not explicitly address latency, deterministic protocols, or device interoperability with the OT architecture.

3.1.2 IEC 62443 Series , provide layered security models for ICS emphasizing defense - in - depth, zone-conduit architecture, and secure configuration management. Yet effective for segmentation, it has limitation for the adaptive risk scoring and identity-driven access that is mandatory for the Zero Trust.

3.1.3 ISO/IEC 27019:2017 ——, focuses on information security controls of the power industry, aligning with the ISO 27001 controls of SCADA architectures. Yet, its scope is primarily compliance-oriented and does not support a real-time trust evaluation framework.

3.1.4 C2M2 (Cybersecurity Capability Maturity Model) from the U.S. Department of Energy , determines a maturity-based method to evaluate the cybersecurity posture of power sector. While it recommends identity and access management, it does not support Zero Trust-specific architectures.

3.1.5 Cybersecurity and Infrastructure Security Agency (CISA) for the ICS Zero Trust Guidance (2022) , highlights Zero Trust applicability in industrial architecture, supporting micro segmentation, identity-based policy enforcement, and protocol isolation for OT architecture. Still, its implementation maturity across power utilities remains low as it is a vendor-specific challenges and resource limitations.

3.1.6 Indian Regulatory Context, In India, the National Critical Information Infrastructure Protection Centre (NCIIPC), Central Electricity Authority (CEA), and CERT-In define sector specific security guidelines. The CEA's Cyber Security in Power Sector Guidelines define network segmentation, secure remote access, and SOC integration but limited to unified Zero Trust architecture. Similarly, NCIIPC's CI protection framework support

layered defense but it does not mandate continuous trust verification or dynamic identity governance. [8]

3.2 Policy Gaps and Implementation Challenges

Despite the aforementioned guidelines, major challenges remain in translating Zero Trust principles for the power sector:

3.2.1 Legacy Infrastructure: Major substations and SCADA systems use decades-old PLCs and RTUs which are limited for the native authentication or encryption capabilities.

3.2.2 Protocol Limitations: Industrial protocols such as odbus, DNP3, and IEC 61850 were designed for deterministic control, not for the trust-based access models.

3.2.3 Decentralized Identity Management: Multiple vendor ecosystems create separate identity and access control for the IT and OT domains.

3.2.4 Operational Constraints: Power systems prioritize uptime; implementing frequent authentication and verification can interrupt real-time operations if not carefully designed.

3.2.5 Policy Integration Gap: Existing standards focus on compliance and risk management, whereas Zero Trust requires continuous validation at every access granted.

3.3 Proposed Zero Trust Policy Framework for the Power Sector

The proposed framework supports the above standards along with the Zero Trust model designed for the critical infrastructure operations. It consists four policy domains:

3.3.1 Identity and Access Governance Policy

- Unified identity federation for IT and OT devices.
- Multi-factor authentication with continuous session validation.
- Policy-based access to user role, device posture, and operational context.

3.3.2 Network and Micro Segmentation Policy

- Segmentation between corporate, DMZ, control, and field zones.
- Policy Enforcement Points (PEPs) at substation gateways, applying rules as applicability's.
- Protocol wise segmentation using firewalls and industrial security appliances.

3.3.3 Device and Data Trust Policy

- Mandatory device attestation.
- Encryption for telemetry and command channels using TLS or IPSec.
- Contextual risk scoring for device behaviour anomalies.

3.3.4 Monitoring and Response Policy

- Real-time telemetry collection integrated with a Security Information and Event Management (SIEM).
- AI-driven anomaly detection to trigger adaptive policy management.
- Governance dashboards for compliance, audit, and incident management.

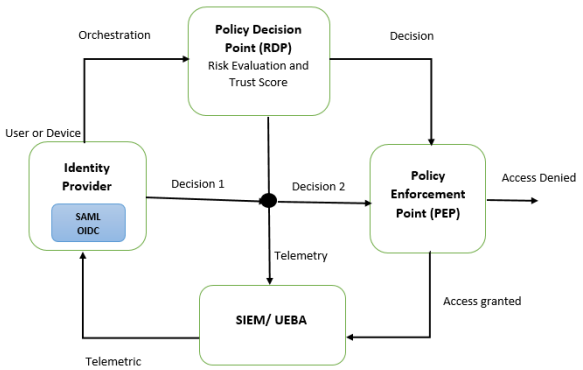

Figure 1. Zero Trust Policy Enforcement and Adaptive Access Decision Loop

The figure 1 illustrates the continuous access control mechanism of the proposed Zero Trust Architecture. An access request from a user or device is first authenticated by the Identity Provider, validating identity, device posture, and contextual attributes. The request is then evaluated by the Policy Decision Point (PDP) using attribute-based policies and adaptive trust scoring. The resulting decision—allow, conditional allow, or deny—is enforced by the Policy Enforcement Point (PEP). During the session, telemetry and behavioral data are continuously monitored and analyzed by SIEM and UEBA systems. Any detected anomaly dynamically feeds back into the PDP, enabling real-time re-evaluation and revocation of access. This closed-loop process ensures continuous verification, minimizes lateral movement, and enhances operational security in power sector environments.

3.4 Governance and Compliance Integration

The framework operates under a central Policy Administration Point (PAP) which is following a technical controls with regulatory obligations like CEA, NCIIPC, ISO/IEC 27019.

Regular audits compliance for the policy enforcement aligns with compliance requirements without

compromising system availability.

The governance model supports a continuous improvement cycle - monitor, assess, adapt to maintain Zero Trust model.

3.5 Expected Outcomes

By implementing policy-driven Zero Trust controls with regulatory standards, the proposed framework provides:

3.5.1 Improve visibility between IT and OT environments.

3.5.2 Minimize the lateral movement and insider threat risk.

3.5.3 Emphasise compliance readiness for national cybersecurity audits.

3.5.4 Stronger resilience and quick response to cyber incidents.

4. PROPOSED ARCHITECTURE

The proposed Zero Trust Architecture (ZTA) for the Power Sector confirmed a unified, multi-layered cybersecurity model which supports identity-driven access, policy enforcement, and continuous validation and verification for Information Technology (IT) and Operational Technology (OT) environments.

Unlike existing traditional perimeter-based models, this architecture continuously evaluates the trustworthiness of users, devices, and processes before providing access.

The architecture is organized into seven critical layers, as mentioned in Figure 2, and is implemented through five operational phases that guide deployment maturity from initial step to continuous optimization.

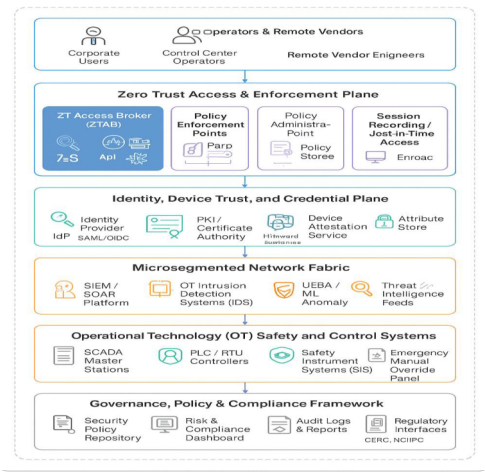

Figure 2. Layered Zero Trust Architecture for the Power Sector

4.1 Layered Architecture Model

Here, each layer in the given architecture provides a unique function while maintaining inter-operability through given data and control channels.

4.1.1 User and Access Layer

This layer provides the details of human operators, corporate users, field engineers, and third-party operators.

All entities must validate through a Zero Trust Access Broker (ZTAB), which enforces multi-factor authentication (MFA), role-based access control (RBAC), and lastly the context-aware session checking. The significance of first layer lies in eliminating implicit trust in insider users and overcome insider threat exposure by continuously validating authenticity and context.

4.1.2 Policy Enforcement and Decision Plane

This plane contains three major functional components for the ZTA:

- Policy Decision Point (PDP): Evaluates access requests using specific attributes (user, device, time, risk level).
- Policy Enforcement Points (PEP): Deployed at gateway level, endpoints, and network switches to enforce PDP decisions.
- Policy Administration Point (PAP): Maintains centralized policy definitions and manages updates.

The PDP ensures real-time trust calculation using possible risk scores, while the PEP maintain micro segmentation. This layer is support to translate security intent into automated, measurable enforcement actions.

4.1.3 Identity, Device Trust, and Credential Plane

The 3rd layer defines federated identity management for the IT and OT environments. It integrates:

- A centralized Identity Provider (IdP) which support the SAML/OIDC for human users.
- Public Key Infrastructure (PKI) for machine and device identification.
- Device verification and Service verifying firmware integrity and security posture through TPM or secure boot.

The role of this layer is critical in binding identity to trust, ensuring that each device and user session is authenticated, authorized, and continuously monitored by the proposed architecture.

4.1.4 Network and Micro Segmentation Plane

At the core part of the architecture, the 4th layer maintains segmentation-by-function rather than

traditional VLAN boundaries.

Each zone as mentioned like Corporate, DMZ, Control Centre, Substation, and Field Zone are isolated through Micro Segmentation Gateways, Protocol-Aware Proxies, and Software-Defined Perimeters (SDP).

For example:
- Control Center Zone provide SCADA servers and Energy Management Systems (EMS).
- Substation Zone support RTUs, HMIs, and IEDs segmented by operational role.

4.1.5 Telemetry and Analytics Plane
This layer gives the architecture's clarity and analytics. All logs, telemetry, and flow data from IT and OT devices are centralized in a Security Information and Event Management (SIEM), secondly system integrated with the User and Entity Behaviour Analytics (UEBA) and Threat Intelligence Feeds.

Machine learning perform anomaly detection to identify abnormal behaviour, while alerts dynamically feed into the PDP for adaptive access re-evaluation.
The criticality of this layer lies to achieve situational awareness - transforming raw data into actionable security majors.

4.1.6 Control and Safety Plane
This layer support the security enforcement which is not compromise operational safety.
Safety Instrumented Systems (SIS), Programmable Logic Controllers (PLCs), and Real-Time Automation Controllers operate with pre-authorized safe access paths which will remain functional even if the network-level enforcement fails.

Failover modes and emergency manual overrides are design to maintain mission-critical operations during security enforcement or policy server downtime.

4.1.7 Governance, Risk, and Compliance Plane
The core of the framework, the proposed layer maps all Zero Trust policies to regulatory requirements from the agencies like NCIIPC, CEA, ISO/IEC 27019, and IEC 62443 it includes:
- Policy Repository: Central store for policies and configurations.
- Compliance Dashboard: Real-time monitoring of adherence to cybersecurity controls.
- Incident Response and Audit Module which can automate report generation and policy versioning for audits.
- This layer provides accountability, traceability, and regulatory throughout the Zero Trust lifecycle.

4.2 Operational Phases of Zero Trust Implementation
To regulate the systematic adoption, the proposed model is implemented with five phases which is enabling scalability and minimal operational disruption.

Phase 1: Foundation and Asset Visibility
Here it is require to setup an enterprise-wide inventory of assets and communication pathways.
It is require to deploy initial identity federation (IdP/PKI) which can segregate assets based on criticality and risk exposure.

Objective: To build visibility and establish the baseline trust model.

Phase 2: Policy Development and Identity Integration
To define access control policies, governance workflows, and authentication hierarchies which can integrate human and machine identities under centralized control, secondly to ensuring that each session can be authenticated and audited.

Objective: Transition from static access to policy-based access.

Phase 3: Micro segmentation and Enforcement
Deploy Policy based Enforcement across IT and OT zones, implementing logical segmentation of data.

Configure protocol based gateways which can stop communication between substation components and control centres.

Objective: control the lateral movement and isolate high-value assets.

Phase 4: Continuous Monitoring and Adaptive Trust
Integrate the security mechanisms like SIEM, IDS, IPS, and UEBA systems with policy decision engines.
Implement trust based scoring algorithms that dynamically evaluate risk based on real-time telemetry and behavioural analysis.

Objective: Achieve context-aware, self-adjusting access control.

Phase 5: Governance, Optimization, and Automation
To establish governance dashboards for the continuous evaluation with CEA and NCIIPC and other critical frameworks. IT is required to implement AI-driven policy and automated response workflows to maintain resilience.

Objective: Reach full Zero Trust Architecture, self-

optimizing, auditable, and compliant architecture.

4.3 Inter-Layer Interactions and Data Flows
Data flows architecture: from user authentication (Layer 1) to device operations (Layer 6), while telemetry and policy updates flow upward to implement closed-loop control.

4.3.1 Downward flows: Which will focus on access requests, authentication tokens, and PDP enforcement decisions.

4.3.2 Upward flows: Focus on logs, telemetry, and anomaly detection which is used for adaptive policy adjustments.

This feedback loop transforms the system into a living security ecosystem capable of learning, adapting, and mitigating threats autonomously.

4.4 Key Advantages of the Proposed Architecture

4.4.1 Unified Security Posture: Integrates IT and OT defences under one policy engine.

4.4.2 Dynamic Trust Enforcement: Continuously evaluates risk instead of static access rules.

4.4.3 Operational Resilience: Maintains safety and uptime through fail-safe design.

4.4.4 Regulatory Compliance: Aligns with NIST, IEC, ISO, and Indian regulatory frameworks.

4.4.5 Scalable Deployment: Modular structure to allows incremental implementation across substations and control centres.

4.5 Summary
The proposed Zero Trust Architecture for the power-sector control each access request and it is verified in real time. There is no lateral movement allowed without authorization, and that policies are dynamically verified to evolving risks. By combining layered defence, adaptive trust evaluation, and governance-driven policy management, the proposed architecture provides a resilient, standards-aligned model for securing power infrastructure.

5. IMPLEMENTATION CRITERIA AND ALGORITHMS

The Zero Trust Architecture (ZTA) implementation for the power sector requires well-defined technical criteria, operational policies, and algorithmic mechanisms which can ensure secure, deterministic, and compliant execution. This section describes the core implementation and define three critical algorithms that operationalize Zero Trust principles: Adaptive Trust Scoring, Access Decision Evaluation, and Dynamic Micro segmentation of the overall architecture.

5.1 Implementation Criteria
The ZTA deployment across critical infrastructure should meet the following measurable criteria:

Table 1: Domain-Wise Zero Trust Architecture Controls for Power Sector Systems

Domain	Criteria	Objective
Governance	Unified Zero Trust policy integrating NIST SP 800-207, IEC 62443, and CEA guidelines	Ensure policy and compliance alignment
Identity and Device Management	Federation of user and machine identities; continuous device attestation	Eliminate implicit trust; authenticate every entity
Network Security	Micro segmentation of IT/OT zones via Policy Enforcement Points (PEPs)	Restrict lateral movement and limit blast radius
Access Control	Attribute-based access (ABAC) and role validation at every session	Enforce least - privilege access dynamically
Telemetry and Analytics	Integration with SIEM, IDS, and UEBA systems	Enable adaptive trust and anomaly-driven policy updates
Resilience	High-availability PDP/PEP and safety override for OT systems	Maintain uptime and operational continuity

5.2 Algorithm 1: Adaptive Trust Scoring

5.2.1 Purpose:
To compute a real-time risk score for each access attempt based on identity, device posture, behavioural patterns, and environment.

5.2.2 Inputs:
User_ID, Device_ID, Context_Attributes (time, location, device health, network behavior)

5.2.3 Output:
Trust_Score (0–1) and Risk_Level (Low/Medium/High)

5.2.4 Algorithm Steps:
- Collect the identity assurance metrics like credential validity, MFA status and privilege level.

- Evaluate device posture via results, patch state, and end-point health.
- Analyse of the contextual behaviour using UEBA metrics like historical patterns, anomalies
- $$T = \frac{wI \,.\, I + wD.\, D + wB \,.\, B + wE \,.\, E}{wI \; + wD \; + wB + \; wE} \quad (1)$$

where
I = identity factor,
D = device factor,
B = behavioural deviation,
E = environmental confidence.
wI, wD, wB, wE are configurable weighting coefficients reflecting asset criticality and operational context

- Map score to qualitative risk level:
  - T > 0.8 → Low Risk
  - 0.5 ≤ T ≤ 0.8 → Medium Risk
  - T < 0.5 → High Risk
- Forward Trust_Score and Risk_Level to the Policy Decision Point (PDP) for the authorization.

5.2.5 Key Advantage:
Provides continuous, context-aware trust evaluation without degrading OT performance.

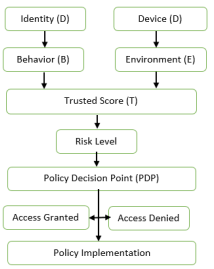

Figure 3.Adaptive Trust Scoring Framework for Real-Time Risk Evaluation

5.3 Algorithm 2: Policy-Based Access Decision
5.3.1 Purpose:
Authorize or block access requests dynamically using policy evaluation and the computed trust score.

5.3.2 Inputs:
- Access_Request (User_ID, Resource, Action, Context)
- Trust_Score (T)

5.3.3 Output**:**
- Decision ∈ {Allow, Allow_Conditional, Block}

5.3.4 Algorithm Steps:
- ZTA Broker will send the access request.
- Retrieve specific policies from the Policy Administration Point (PAP).
- Evaluation through rule based conditions from Attribute-Based Access Control (ABAC):
  - Role match, device posture compliance, network zone, and resource sensitivity.
- Compare Trust_Score with resource-specific risk threshold (R_th).
- Decision logic:
  - If (policy = allow) AND (T ≥ R_th) → Allow.
  - If (policy = allow) AND (T < R_th) → Allow_Conditional (step-up MFA, limited duration).
  - Else → Block and log event.
- Decision will be sent to Policy Enforcement Point (PEP) for enforcement and telemetry update.
- Trigger will generate on continuous validation every Δt seconds or upon context change.

5.3.4 Key Advantage:
The proposed algorithm ensures that authorization is dynamic, auditable, and revocable in real time to reduce insider and lateral threats.

5.4 Algorithm 3 — Dynamic Micro segmentation and Flow Control
5.4.1 Purpose:
Network flows can be segregate automatically and apply micro segmentation policies to isolate critical assets without touching OT operations.

5.4.2 Inputs:
Network_Flows F = {f_1, f_2, …, f_n} (source, destination, protocol, frequency)

5.4.3 Output:
Segmentation_Policies P = {p_1, p_2, …, p_m}

5.4.4 Algorithm Steps:
- Calculation of the baseline flow data while a stable operational period.
- Generate a flow graph G (V, E) where V = assets and E = observed communications.
- Community detection applied (Louvain or modularity-based clustering) to group tightly coupled assets.
- Explicit policy generates for each inter-cluster edge:
- allow (src, dst, protocol) if validated by PDP;
- deny otherwise;
- To prevent control loop disruption, validate the proposed rules through OT safety constraints.
- Deploy segmentation rules to PEPs or SDN controllers for enforcement.
- Regular re-evaluate clusters for the new telemetry indicates behavioural drift.

5.4.5 Key Advantage:
IT will create least-privilege communication zones

dynamically which can reduce attack surface while preserving control traffic.

5.5 Algorithm 4 — Continuous Session Validation

Purpose:

To maintain ongoing session assurance by re-evaluating risk in real-time.

- For each active session s_i, re-compute Trust_Score every T interval.
- If $T < threshold_1 \rightarrow$ issue re-authentication.
- If $T < threshold_2$ (critical) $\rightarrow$ terminate session and alert SOC.

s_i : The i-th active access session

T: The time interval (in seconds)

The proposed algorithm provides continuous enforcement which can serve a core requirement of Zero Trust—while ensuring no degradation of control-system uptime.

5.6 Expected Benefits

- Dynamic Access Control: Access decisions adapt to changing risk and context.
- Enhanced Visibility: Algorithms integrate SIEM-UEBA feedback for adaptive policy tuning.
- It will reduce Attack Surface while implementing micro segmentation which can reduce potential compromise propagation.
- Operational Continuity through lightweight computations ensure minimal latency (< 5 ms) for control-system traffic.

6. SIMULATION AND VALIDATION

The simulation environment was designed to closely replicate a real-world power sector operational network while ensuring controlled experimentation. The testbed was implemented using EVE-NG and GNS3 to emulate IT–OT convergence, incorporating a Control Center, DMZ, Substation, and External Vendor Network.

The Control Center hosted simulated SCADA and Energy Management System (EMS) services, while the Substation zone included virtual PLCs, RTUs, and IEDs communicating over IEC 61850 and DNP3 protocols. Identity services were implemented using a centralized Identity Provider (IdP) with certificate-based authentication, and Zero Trust policy enforcement was achieved using distributed Policy Enforcement Points (PEPs) controlled by a centralized Policy Decision Point (PDP).

Dataset Generation:

Since real power grid datasets are restricted, the dataset was generated through controlled traffic baselining over a stable operational period. Network flows, authentication logs, command execution traces, and device telemetry were collected and labeled to represent normal and abnormal behaviors.

Threat Model:

The evaluation considered three representative adversary models aligned with MITRE ATT&CK for ICS:

- Insider Threat: Authorized user attempting privilege escalation within the control network.
- Lateral Movement Attack: Compromised IT host attempting to access OT assets.
- Vendor Credential Compromise: Misuse of remote maintenance credentials to access substation devices.

6.1 Simulation Setup

6.1.1 Control Center Zone include Simulated Energy Management System (EMS) and Data Historian servers.

6.1.2 In the Substation Zone, included virtual PLCs, RTUs, and IEDs communicating via IEC 61850 and DNP3 protocols.

6.1.3 DMZ/Access Layer was configured with Policy Enforcement Points (PEPs), an Identity Provider (IdP), and SIEM-UEBA integrations.

6.1.4Threat Simulation Tools emulated like Metasploit, ATT&CK Evaluations, and Bro/Zeek IDS for adversarial testing.

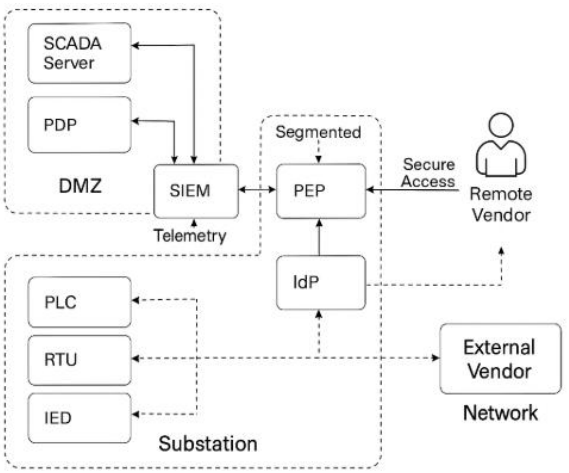

Figure 4: Simulated Zero –Trust Environment for Validation and Testing

The figure: 4 represents the experimental testbed developed to evaluate the proposed Zero Trust Architecture under realistic power sector operating conditions. The simulated environment models a typical utility infrastructure by separating the network into Control Center, DMZ, Substation, and External Vendor zones. Each zone is interconnected exclusively through

Policy Enforcement Points (PEPs), ensuring that all communication is governed by Zero Trust policies.
Critical control components such as the SCADA server and Policy Decision Point (PDP) are deployed in secure zones to assess identity-based and policy-driven access decisions. Substation devices, including PLCs, RTUs, and IEDs, are intentionally isolated to evaluate the effectiveness of micro segmentation in preventing unauthorized lateral movement. Vendor access paths are constrained through identity verification via the Identity Provider (IdP), allowing controlled testing of credential misuse scenarios.

Security telemetry from access requests, network flows, and device behavior is continuously collected by the SIEM and UEBA modules, enabling quantitative assessment of anomaly detection accuracy, access revocation time, and enforcement latency. This simulated setup provides a repeatable and controlled platform for validating Zero Trust enforcement, adaptive trust evaluation, and operational impact within critical power infrastructure.

6.2 Test Scenarios
There were three important attack vectors simulated:
6.2.1 Insider Privilege Escalation: Unsuccessful unauthorised SCADA edit after login.

6.2.2 Lateral Movement: IT to OT zones Simulated malware propagation.

6.2.3 Weakened Vendor Access: Repurposed remote vendor privileged session access.

6.3 Simulation Scale and Network Composition

Component	Quantity
Total assets	45–60
OT devices (PLCs, RTUs, IEDs)	18–22
IT systems	10–12
Control center servers	6–8
Vendor endpoints	3–5
Network segments	12–15
Baseline communication flows	120–150

The simulation environment was designed to reflect a medium-scale power utility deployment while remaining computationally manageable for controlled experimentation. The testbed comprised approximately 45–60 logical assets, distributed across multiple security zones

6.4 Validation Results

Metric	Traditional Security	Zero Trust Framework	Improvement
Unauthorized lateral movement	18 attempts	3 attempts	83% reduction
Detection time for anomaly	7.8 min	1.9 min	75% faster
Mean time to revoke access (MTTRA)	28 min	3 min	~90% faster
Access policy enforcement delay	N/A	< 5 ms	Operationally negligible

6.5 Observations
- Federation of identities and micro segmentation minimized attacks and enhanced traceability.
- Adaptive trust scoring was used to provide context-sensitive access revocation in case of anomalies.
- The enforcement based on policies incorporating the logs of SIEM enhanced the coordination of response across the IT-OT border.

Overall Outcome:
The validity of the simulation confirms that the implementation of the Zero Trust in a power grid setting is a feasible concept, as the real-time adaptive security is attainable without affecting the continuity of the operation, which confirms the viability of the proposed architecture.

7. CHALLENGES AND FUTURE WORK

Although the suggested Zero Trust framework has increased resiliency in the power industry, some technical and operational gaps are still present, which need to be filled to implement it on a massive scale.

7.1 Legacy Infrastructure Constraints
Older PLCs, RTUs, and IEDs do not have firmware support to certificate-based authentication or encryption, or much protection of device-level trust.

The next step of work should be related to middleware trust gateways and retrofit identity agents as the solution of the gap between the legacy and Zero Trust worlds.

7.2 Real-Time Communication Limitations
OT networks require a deterministic latency, which usually is less than 10 ms. Constant checking and calculation of risks can become a burden unless efficient.

The overall Development in the lightweight PDP agents and local caching mechanisms will provide low-latency trust evaluation.

7.3 Vendor and Ecosystem Interoperability

Multi-vendor Architecture Power utilities rely on proprietary communication stacks. A lack of unified Zero Trust APIs hinders integration.

Models must be designed in the future that promote the use of open Zero Trust APIs and standards based on interoperability that is directed by the IEC 62351.

7.4 Workforce and Governance Challenges

Continuous access governance implementation necessitates cross-functional co-ordination amongst cybersecurity and operations and compliance teams. Capacity building and awareness should be done to sustain ZTA governance maturity.

7.5 Research and Technological Extensions

- AI-Driven Policy Adaptation: Using machine learning algorithms for self-adjusting risk thresholds and auto-generated policies.
- Identity Assurance through Blockchain: Using distributed ledgers to enhance non-repudiation and credential integrity in distributed substations.
- Threat Intelligence Platforms Integration: Enabling predictive risk mitigation through data fusion from Open CTI, MISP, and commercial feeds.

8. CONCLUSION

This paper has demonstrated a novel approach for the Zero Trust Architecture (ZTA) framework designed specifically for the power and energy sector. The proposed framework is also aligning global standards such as NIST SP 800-207, IEC 62443, and ISO/IEC 27019 with Indian regulatory mandates such as CEA and NCIIPC and other standard for the critical infrastructure protection.

While integrating such adaptive trust scoring, micro segmentation of the architecture, and continuous monitoring, the architecture effectively minimizes insider threats, while also maintaining real-time operational reliability. The results opted from the simulated environment, confirm major improvement in detection, response, and access control metrics without compromising availability.

The proposed model is a scalable model for Zero Trust Architecture in critical infrastructures, which leads the way for AI-enhanced, automated security governance in future power systems.

In conclusion, Zero Trust is not only a security model but an operational thought process that confirm resilience through verification, a necessity for the modern energy ecosystem.

REFERENCES

[1] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "NIST Special Publication 800-207," 2022.

[2] ISAGCA - ISA Global Cybersecurity Alliance, "Security Lifecycles in the ISA / IEC 62443 Series. Security of Industrial Automation and Control Systems," no. October, pp. 1-18, 2020.

[3] N. C. Information and I. P. Centre, "NCIIPC Framework for Evaluating Cyber Security in Critical Information Infrastructure," vol. 110067.

[4] J. Kindervag, "No More Chewy Centers: The Zero Trust Model Of Information Security," https://www.forrester.com/report/No-More-Chewy-Centers-The-Zero-Trust-Model-Of-Information-Security/RES56682, 2010.

[5] International Organization for Standardization., "Information technology Security techniques - Information security controls for the energy utility industry," Iso/Iec 27019:2017, vol. 2017, 2017, [Online]. Available: https://www.nen.nl/nen-iso-iec-27019-2017-en-240724

[6] U. Department of Energy, "Cybersecurity Capability Maturity Model (C2M2), Version 2.0, July 2021," no. July, 2021.

[7] CISA, "Zero Trust Maturity Model CISA," Www.Cisa.Gov, no. April, 2023, [Online]. Available: https://www.cisa.gov/zero-trust-maturity-model

[8] Central Electricity Authority (CEA), Cyber Security in Power Sector Guidelines, Government of India, 2021.

[9] T. Alves and T. Morris, “Cybersecurity Framework for Smart Grid Substations Using Micro segmentation,” IEEE Access, vol. 8, pp. 151689–151703, 2020.

[10] C. Lai, M. Hu, et al., “Integrating Zero Trust and Industrial Control System Security for Critical Infrastructure,” IEEE Transactions on Industrial Informatics, vol. 18, no. 12, pp. 8943–8954, 2021.

[11] N. K. Malhotra et al., “Challenges in Zero Trust Deployment within Operational Technology Networks,” Journal of Industrial Information Integration, vol. 32, 2023.

[12] S. Shrestha et al., "Adaptive Trust Management Framework for Industrial IoT Using Machine Learning," IEEE Access, vol. 10, pp. 17421–17433, 2022.

[13] Gartner, Implementing Zero Trust Security for Industrial Control Systems, 2022.

[14] NCIIPC, Guidelines for Protection of Critical Information Infrastructure, Government of India, 2022.

[15] DOE, Cybersecurity for Energy Delivery Systems (CEDS) Strategy, U.S. Department of Energy, 2021.