INDUSTRIAL CONTROL SYSTEM SECURITY IMPLEMENTATION FOR A MAJOR POWER SECTOR CLIENT – TRINITY TOUCH PVT. LTD.

INDUSTRY

RENEWABLE ENERGY

STANDARDS

IEC 62443, NIST 800-82, NERC CIP, ISO 27001

PRIMARY SECTOR

POWER SECTOR

PROJECT TYPE

INDUSTRIAL

LOCATION

MAHARASHTRA

INDIA

OFFERED SERVICE

OT SECURITY GAP ASSESSMENT, CONFIGURATION REVIEW, POC OF IDS SECURITY TOOL, Vulnerability Assessment

CLIENT PAIN POINT & CHALLENGES

The client experienced a critical server failure in the OT environment, where the primary system became corrupted and stopped functioning. Due to the absence of redundancy and backup mechanisms, the system was unable to handle operational load, leading to a complete disruption of services.

The overall OT infrastructure lacked proper cybersecurity controls and was not aligned with regulatory requirements such as ***Central Electricity Authority (CEA)*** *cybersecurity guidelines.*

In addition, flat network architectures and the convergence of IT and OT environments increase the risk of lateral movement once an attacker gains access.

Remote access required for vendors and maintenance teams often introduces additional vulnerabilities if not properly secured. These challenges are compounded by complex compliance requirements, dependence on third-party vendors, and the potential for severe operational, safety, and financial impacts in the event of a cyber incident.

EXISTING SET UP

- *No data backup or disaster recovery mechanism was implemented.*
- *No firewall or network security controls deployed in the OT network.*
- *Use of fully utilized unmanaged switches, leading to performance bottlenecks.*
- *No proper network segmentation (IT/OT/DMZ separation missing).*
- *Absence of monitoring, logging, or intrusion detection systems.*
- *Manual dependency on vendors for system restoration and software reinstallation.*

IMPACT OF THE PROBLEM

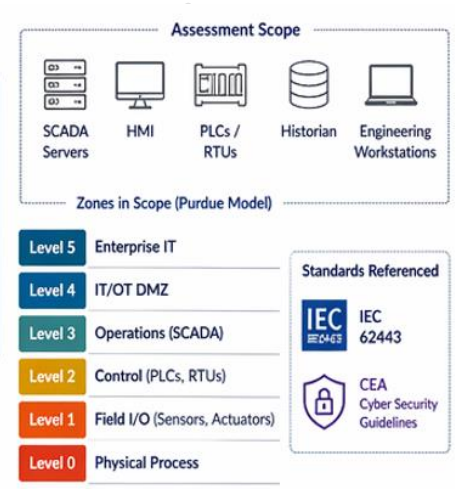
The lack of basic cybersecurity and infrastructure controls resulted in:

- ***Operational Downtime:*** *Complete halt of plant operations during server failure.*
- ***Increased Recovery Time****: Vendors had to be called onsite to reinstall all applications and restore systems.*
- ***Data Loss Risk****: No backup resulted in potential loss of critical operational data.*
- ***Performance Issues****: Overloaded switches and lack of load handling capability.*
- ***Safety & Reliability Concerns****: Unstable OT environment impacting plant reliability.*

- ***Financial Impact**: Increased cost due to downtime and repeated vendor dependency.*
- ***Compliance Gap**: Non-alignment with CEA cybersecurity guidelines.*

OBJECTIVE AND SCOPE

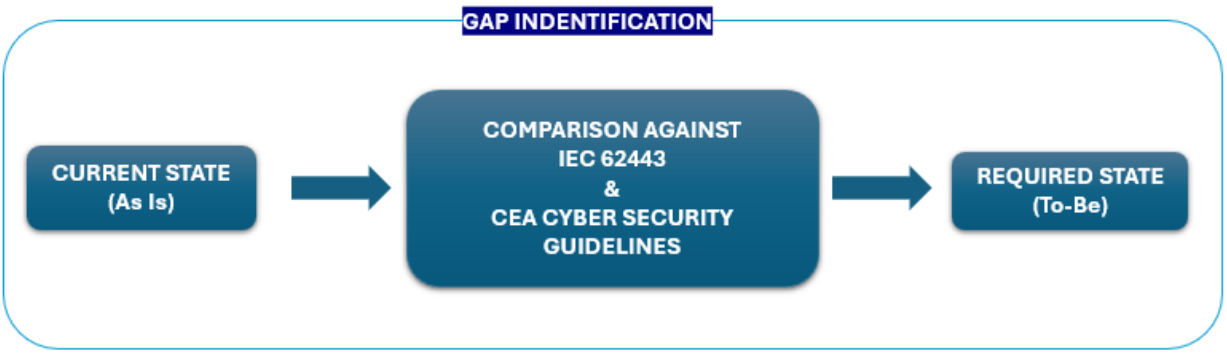
- *Evaluate the current OT security environment to understand the plant's cyber risk exposure, maturity level, and alignment with industry standards.*
- *Detect existing loopholes, misconfigurations, exposed services, weak access controls, and other potential attack vectors across the OT infrastructure.*
- *Assess the feasibility, performance, and operational impact of deploying a dedicated OT cybersecurity monitoring solution within the power plant environment.*



TRINITY TOUCH OT CYBERSECURITY SOLUTION

1. GAP ASSESSMENT OVERVIEW

This diagram illustrates a structured approach to evaluating the current SCADA/OT environment against industry standards such as IEC 62443 and CEA Cyber Security Guidelines. It covers key stages including scope definition, asset and architecture review (Purdue model), security controls assessment, backup and monitoring validation, gap identification, and risk prioritization. The outcome provides a clear view of the existing security posture along with a prioritized remediation roadmap to enhance system security, resilience, and compliance.



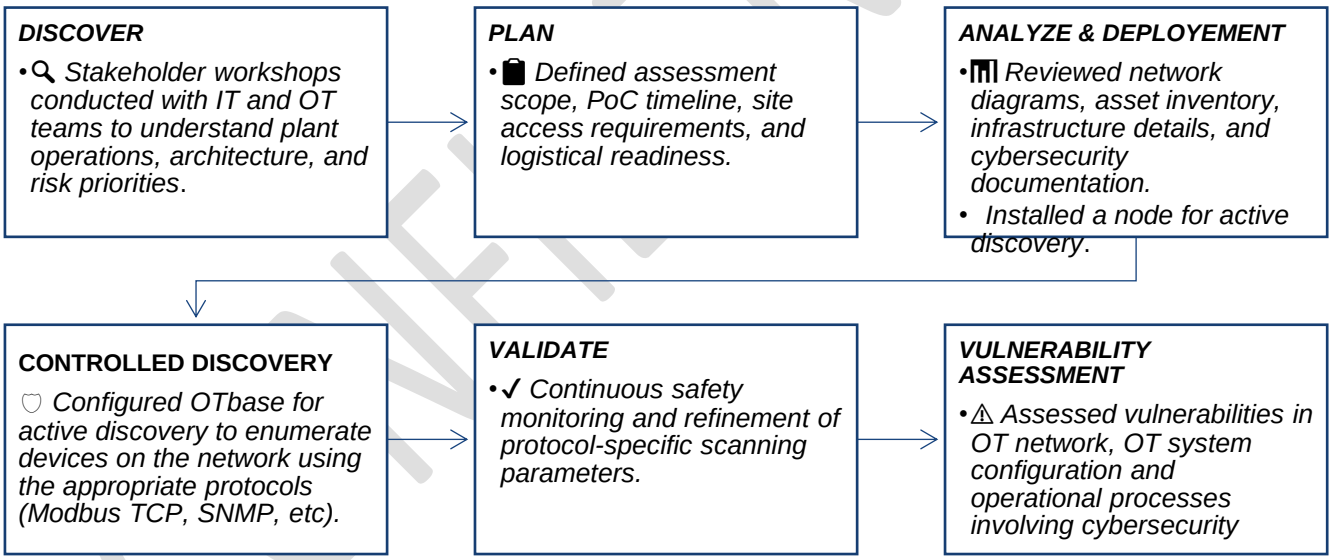
2. TRINITY TOUCH OT SECURITY (IDS) PRODUCT OVERVIEW

*The **TRINITY TOUCH OT security IDS solution** was selected based on its strong alignment with industry standards such as IEC 62443 and CEA Cyber Security Guidelines, along with its ability to address key gaps identified during the assessment*

IN-SCOPE ENVIRONMENT

The assessment scope for this PoC was limited to the client's 10 MW plant environment, covering only the defined operational technology and network infrastructure authorized for testing. This included 15 identified network-connected devices, associated systems, and supporting infrastructure located onsite where implementation activities were performed. In cybersecurity engagements, the scope defines the exact assets, systems, and boundaries to be evaluated so efforts remain focused and relevant to objectives.

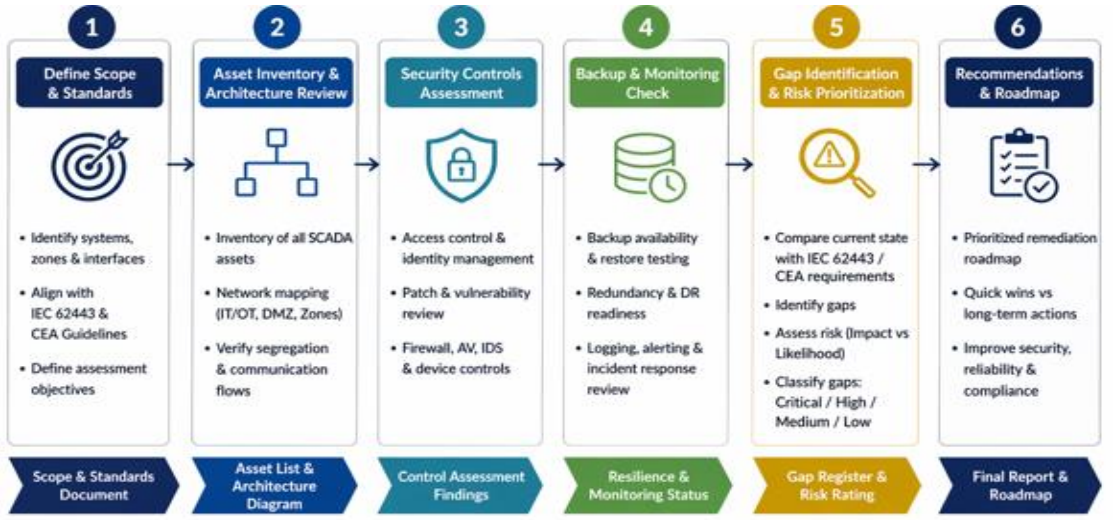
SOLUTION APPROACH & METHODOLOGY FRAMEWORK



SOLUTION CUSTOMIZATION & OPTIMIZATION

- *IDS Rule Tuning: Optimized for OT protocols (Modbus, IEC) to reduce false positives*
- *Asset Baselining: Identified and profiled PLCs, HMIs, and SCADA systems*
- *Purdue-Based Monitoring: Configured zone-wise visibility and alerts*
- *DMZ Enhancement: Added server to support applications and ensure performance*
- *Secure Remote Access: Implemented RBAC and monitored jump server access*
- *Backup Optimization: Scheduled backups for critical systems based on operations*
- *Dashboard & Alerts: Prioritized alerts with customized monitoring views*
- *CEA Compliance: Aligned logging and reporting with regulatory requirements*

PRODUCT OVERVIEW/FEATURES:



KEY FEATURES:

- ***Real time threat detection***: *monitors network traffic 24/7 to identify attacks and anomalies.*
- ***Asset visibility***: *understand industrial protocols (IEC 61850, Modbus, DNP3, OPC, etc.) and identify critical assets.*
- ***Behavior anomaly detection***: *Detects abnormal behavior and policy violations in OT and IT environment.*
- ***Instant Alerts and notifications***: *Sends real time alerts to SOC/engineers for quick response.*
- ***Forensics and Incident analysis***: *Provides detailed logs, reports and traffic analysis for root cause investigation.*
- ***Integration and Scalability***: *Seamlessly integrates with SIEM, firewalls and other security tools. Scales with plant infrastructure.*

THE IMPLEMENTATION WAS CARRIED OUT IN A PHASED APPROACH OVER 45 DAYS TO ENSURE MINIMAL DISRUPTION TO PLANT OPERATIONS.

KEY EMERGING OBSERVATIONS

Below are the Critical Emerging Observations.

Unrestricted Internet & Perimeter Exposure

We identified that the SCADA Server and critical network devices have unrestricted outbound internet access. Furthermore, the leased-line router has an internet-exposed interface directly connected to the client-managed TP-Link.

***The Risk**: This creates a direct path for external threats to reach critical assets and allows for potential data exfiltration. Additionally, the use of public DNS leaks internal network metadata to the public web.*

Compromised Account Management (IAM)

Routine tasks are currently performed using accounts with local admin privileges. Most critically, the SCADA Server is accessed via a shared Service Provider Microsoft account.

***The Risk:** Sharing administrative accounts*

Insecure Remote Access Mechanisms

Third party remote access tool are currently installed and routinely used for remote access to the plant SCADA Server.

The Risk: These cloud-based tools bypass traditional perimeter security and lack the granular access controls, multi-factor authentication (MFA), and audit logging required for industrial environments.

Improper Network Segmentation & Hotspots

The network relies on unmanaged switches, preventing VLAN segmentation. Additionally, the Win11 Pro (Security Server) was found with the "Mobile Hotspot" feature enabled.

Lack of Synchronization & Logging

An on-site GPS clock is present but not utilized by the assets. Furthermore, Syslog is not configured, and local device logging is inconsistent.

***The Risk:** Without time synchronization, correlating events across devices during an incident is painful and slows down the Incident Response. The lack of centralized logging prevents proactive monitoring and effective forensic analysis.*

Deficient Backup & Governance

Routine tasks are currently performed using accounts with local admin privileges. Most critically, the SCADA Server is accessed via a shared Service Provider Microsoft account.

***The Risk:** Ad-hoc backups risk extended downtime or total data loss in the event of a failure or ransomware attack. The lack of GPOs means there is no centralized enforcement of password complexity or security policies. no proper backup plan = high chance of downtime + permanent data loss.*

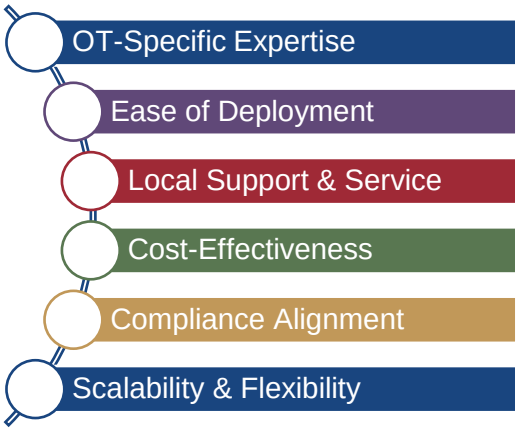
We conducted a gap assessment aligned with NIST SP 800-82 and IEC 62443 standards. The current compliance score is 2% out of 20%, which indicates a high-risk posture for a critical site.

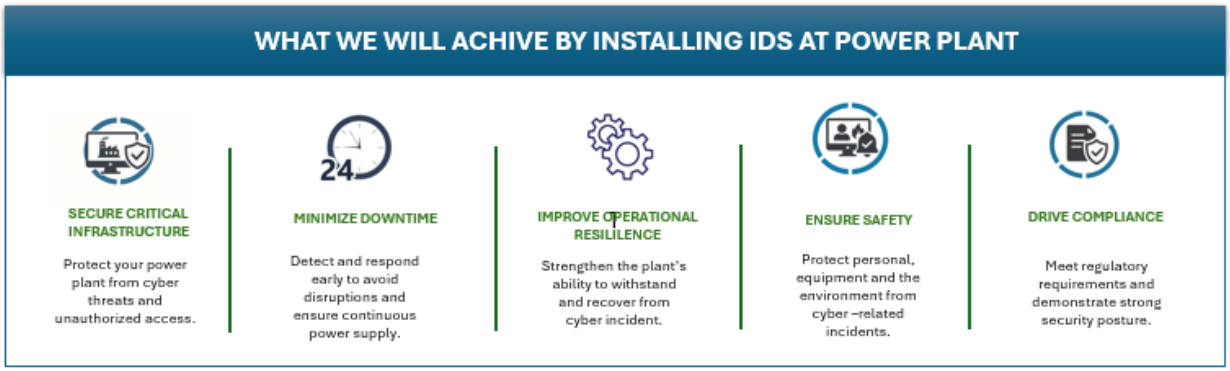
VENDOR SELECTION & COMPETITIVE EVALUATION

Clients had evaluated multiple OT cybersecurity solution providers before finalizing Trinity Touch.

Competitor brands considered

1. *Nozomi Networks.*
2. *OTBase Security*





TECHNICAL ADVANTAGES

- **Non- Intrusive Deployment (No impact on operation)**
- **OT-Specific detetction (with low false positives)**
- **Scalable Architecture (align with pPerdue model)**
- **Easy integration (with existing SCADA/OT steup)**

EASE OF INSTALLATION

- **Quick deployment** using SPAN/mirror ports
- **Minimal changes** to exiting network
- **User-freindly interface** for operators
- **Simplified monitoring** and Reporting

RECOMMANDATION

- *Deploy a perimeter firewall with a default-deny outbound policy and use an internal DNS forwarder.*
- *Replace third-party remote tools with secure VPN or Zero Trust access using MFA.*
- *Use managed switches to enable VLAN segmentation and disable hotspot features.*
- *Synchronize all devices with a trusted time source and send logs to a central Syslog server.*

OVERALL IMPACT

Installing OT security tools in a power plant improves security and keeps operations running smoothly. It helps detect threats early, reduces downtime, and provides better visibility of all systems.

Secure network design and controlled access lower risks, while backup systems ensure quick recovery. Overall, it makes the plant safer, more reliable, and compliant with regulations.

ENGAGEMENT DELIVERABLES

- ✓ *Complete OT asset inventory*
- ✓ *Risk & Vulnerability Identification*
- ✓ *Improved Network Segmentation*
- ✓ *Early threat detection and abnormal behavior*
- ✓ *Improved secure remote access monitoring*
- ✓ *Reduction of attack surface and exposures of risk*
- ✓ *Enhanced incident response capability*
- ✓ *Support for compliance requirement.*

REPORTING OUTCOMES

All reports and remediation recommendations were tailored to align with the customer's operational environment, infrastructure architecture, and development framework. The following deliverables were provided as part of the engagement:

- ❖ ***Weekly Status Reports**: Included activity updates, log analysis summaries, observations, and progress tracking.*
- ❖ ***Gap Assessment Report**: Identified compliance gaps against applicable security standards and best practices.*
- ❖ ***Vulnerability Management Report**: Documented discovered vulnerabilities, risk ratings, and prioritized remediation actions.*
- ❖ ***Field Implementation Report**: Summarized onsite activities, configurations performed, and validation results.*

CONCLUSION

The PoC demonstrated that implementing an OT security solution provides immediate visibility into assets, vulnerabilities, and network risks. It revealed critical security gaps and enabled the team to prioritize remediation and strengthen controls without impacting operations. The results confirmed the

value of proactive monitoring and supported the case for full-scale deployment to improve overall security posture.

This visibility allowed the plant team to prioritize remediation actions, improve segmentation planning, and strengthen defensive controls without impacting operations.

Overall, the PoC confirmed that implementing a dedicated OT security platform significantly enhances situational awareness, reduces attack surface, and supports compliance readiness.

FEEDBACK OUTCOME

The client was surprised by the number of previously unknown vulnerable and unmanaged devices discovered. They acknowledged that the tool provided their first real view of the plant's security posture and expressed appreciation for the visibility and risk transparency delivered.