iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 Issue: I Month of publication: January 2026

DOI: https://doi.org/10.22214/ijraset.2026.77028

Proactive Modernization of OT Network Backbone through Replacement of Legacy Cisco Switches in a Thermal Power Plant

Anupam Patnaik
Hindalco Industries Limited, India

***Abstract:** Modern thermal power plants are increasingly integrating Operational Technology (OT) networks with higher-level analytics platforms such as OSI PI and cloud-based systems to support digital transformation initiatives. However, such integrations significantly increase cybersecurity exposure, particularly when legacy and unsupported network infrastructure is retained.*

This paper presents a lifecycle-driven and cyber-aware modernization of an OT network backbone involving the replacement of legacy Cisco Catalyst 2960 Series switches with Cisco Catalyst 1300 Series and Catalyst 9200L switches. The upgrade was necessitated by End-of-Sale (EOS) and End-of-Support (EoS) declarations, coupled with the introduction of OSI PI data flow from DCS through Kepware servers to cloud platforms. In addition to infrastructure upgrade, a SCADA-based network health monitoring system was developed to visualize the availability of redundant networks (NET-A and NET-B), enabling early detection of network degradation or failure. All switch configuration, testing, and commissioning were performed in-house through self-learning, without reliance on external vendors. Enhanced network segmentation, and security policies were implemented to mitigate cybersecurity risks while ensuring performance and scalability. The results demonstrate improved reliability, security posture, and internal capability development, providing a repeatable framework for OT network modernization.

I. INTRODUCTION

The OT network backbone of thermal power plants plays a critical role in ensuring uninterrupted communication between Distributed Control Systems (DCS), SCADA servers, historians, and auxiliary systems. Traditionally, such networks were isolated and built with long-lived hardware. However, the adoption of digital platforms such as OSI PI historians, Kepware OPC servers, and cloud analytics has transformed OT networks into interconnected environments with significantly higher cybersecurity exposure.In the present system, the OT network relied on Cisco Catalyst 2960 Series switches, which have reached EOS and EoS as per OEM lifecycle announcements. Continued operation of these devices posed operational, cybersecurity, and business continuity risks—especially with active DCS-to-cloud data transfer via OPC Servers.

To address these challenges, a proactive and structured network modernization program was initiated, replacing legacy switches with Cisco Catalyst 1300 and 9200L series switches. To enhance both infrastructure reliability and operational visibility, the modernization program included not only switch replacement but also the development of dedicated SCADA pages to monitor real-time network health status for NET-A and NET-B. This enabled operators and maintenance teams to quickly identify network issues and initiate corrective actions. The complete activity, including configuration and commissioning, was executed internally, emphasizing self-reliance and sustainable capability development.

A. Problem Faced

1) Legacy Cisco Catalyst 2960 switches declared EOS and EoS by OEM.
2) Introduction of OSI PI connectivity via Kepware to cloud, increasing cyber exposure.
3) Lack of security patches and modern security features on legacy switches.
4) Risk of lateral movement across OT network due to poor segmentation.
5) Aging hardware increasing probability of network outages.
6) High dependency on vendors for configuration and troubleshooting.
7) Limited scalability to support future digital initiatives.

B. Root Cause

The root cause was the continued use of unsupported legacy network infrastructure in an OT environment that had evolved to include cloud connectivity. Secondary root causes included:

1) Absence of earlier lifecycle-driven network planning
2) Inadequate cybersecurity controls for converged OT–IT data flows
3) Dependence on vendor-led execution models rather than internal capability

II. METHODOLOGY

1) Management of Change (MOC) Approval :- A formal MOC document was prepared and approved by top management prior to execution. It covered:

- Technical specifications of new switches
- Cybersecurity risk assessment (DCS–OSI PI–Cloud)
- Migration, rollback, and validation strategy

2) Life Cycle and Cyber Risk Assessment :-OEM lifecycle notifications and cybersecurity risks associated with cloud connectivity were assessed in line with IEC 62443 and NIST SP 800-82 principles.

3) Network Architecture Review :- Existing OT network topology, including DCS, OSI PI, Kepware servers, and internet-facing zones, was documented.

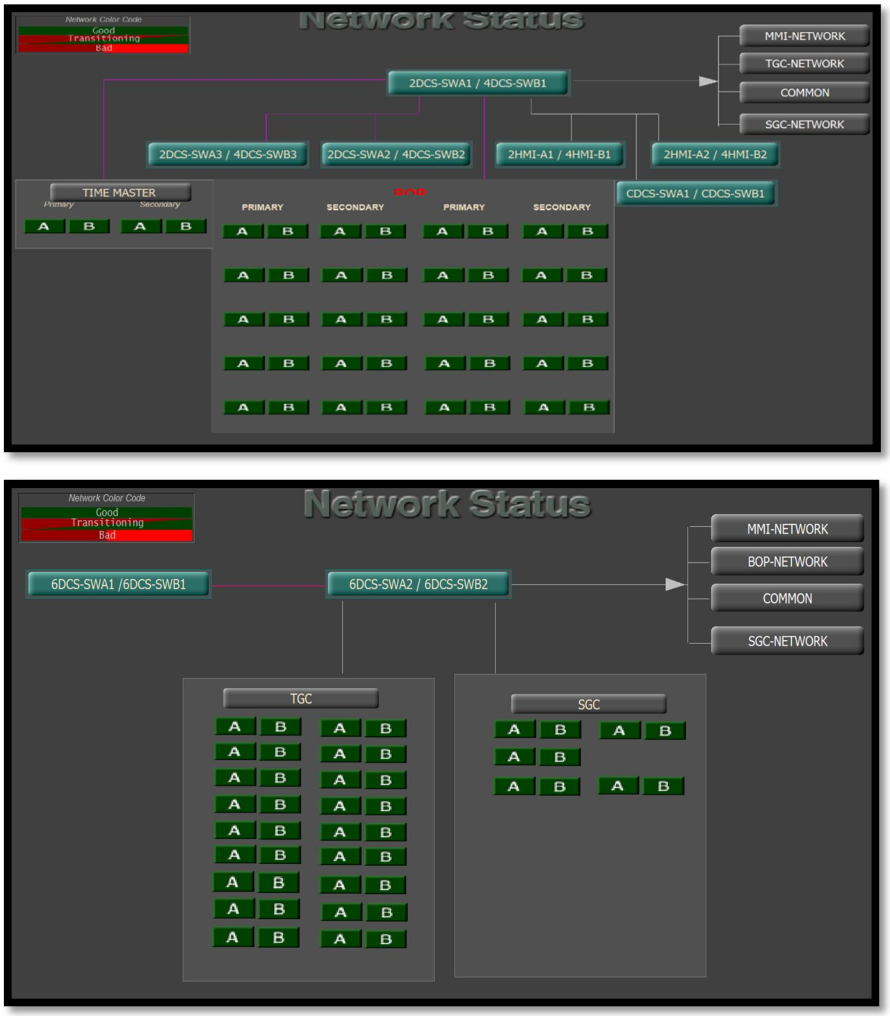
4) Self Learning and Configuration Development :- All switch configurations were developed in-house through self-learning and hands-on validation, including:

- Access control and port security
- Configuration of IP address
- Self Leaning and self development in configuring a New Network Switch from scratch.
- Healthiness of all Network Ports and Configuration.

5) Phased Migration and Commissioning :- Switch replacement was carried out unit-wise and panel-wise during planned opportunity windows, strictly adhering to the approved MOC.

Above is New Network Switch installed (CISCO Catalyst 9200) for Status Monitoring of NET-A and B for DCS

Below is SCADA Developed for Switch Status Monitoring of NET-A and B for DCS



QC Tools

- Management of Change (MOC) – Governance, approval, and compliance.
- Risk Assessment Matrix – Operational and cybersecurity risk evaluation.
- Fishbone (Cause-and-Effect) Analysis – Identification of failure and security contributors.
- Pareto Analysis – Prioritization of critical network segments.
- Checklist-Based Validation – Configuration, connectivity, and security compliance.

III. **IMPLEMENTATION** RESULTS

1) Successful replacement of legacy switches across **six operational units (~60 switches)**.
2) Secure and stable DCS → OSI PI → Kepware → Cloud data flow achieved.
3) Improved network performance with reduced latency and congestion.
4) Enhanced cybersecurity posture through segmentation and supported firmware.
5) Zero unplanned outages during migration.
6) Complete elimination of vendor dependency for configuration and commissioning.
7) Significant improvement in internal OT networking competence.
8) Real-time monitoring of **NET-A and NET-B** network health through dedicated SCADA graphics.
9) Faster fault identification and Improved operator awareness and proactive response to communication issues.

A. Lession Learned

1) OT networks must evolve alongside digital and cloud integration initiatives.
2) Legacy hardware significantly amplifies cybersecurity risk in connected environments.
3) Formal MOC processes are essential for safe OT changes.
4) Self-learning and hands-on execution build sustainable internal capability.
5) Proactive lifecycle-driven upgrades prevent crisis-driven failures.

B. Benefits of Proposed Change

1) Improved Network Performance: Faster throughput and reduced latency supporting real-time control traffic.
2) Enhanced Security: Compliance with modern cybersecurity standards and availability of security patches.
3) Scalability and Future-Proofing: Infrastructure ready for future expansion and digital transformation initiatives.
4) Improved User Experience: Seamless connectivity for DCS, SCADA and enterprise applications.

C. Business and Operation Impact of Not Upgrading

1) Increased risk of network outages due to aging and unsupported hardware.
2) Non-compliance with cybersecurity standards and audit requirements.
3) Higher maintenance costs caused by scarcity of spares and longer recovery times.
4) Increased dependency on emergency vendor support.
5) Potential impact on plant availability and business continuity.

IV. CONCLUSION

This project demonstrates that secure and reliable OT network modernization is essential when integrating DCS systems with historians and cloud platforms. By replacing legacy, unsupported switches with modern, secure alternatives and executing the project entirely in-house, the organization significantly improved its cybersecurity posture, reliability, and scalability.The structured, MOC-driven and self-executed approach presented in this paper provides a practical and repeatable framework for industrial facilities undertaking OT network upgrades in the era of digital transformation. Additionally, the integration of SCADA-based network health monitoring for redundant networks (NET-A and NET-B) enhanced operational visibility and accelerated fault detection. By providing intuitive graphical dashboards within the control room environment, operators gained real-time insight into network availability, further strengthening system resilience.

REFERENCES

[1] Cisco Systems – Product Lifecycle and Security Advisory Documentation (End-of-Sale and End-of-Life Announcement for the Cisco IOS Software and DWP dot1x Licenses for Catalyst 2960 Series Switches - Cisco)
[2] IEC 62443 – Industrial Automation and Control Systems Security.
[3] NIST SP 800-82 – Guide to Industrial Control System Security.
[4] OSIsoft PI System Architecture and Security Guidelines.