PROACTIVE™
Enhancing Digital Experience

OT/IT Segmentation Reference Architecture for Indian Manufacturing: A Field Guide for CIOs, Plant IT Heads, and Cyber Security Leaders.

Purdue model. IEC 62443. Legacy OT protection. Multi-vendor plant floors. Ransomware defence. Schedule M and TISAX evidence. Costed to Indian market bands.

Version 1.1 · Updated August 2026 ·

Reflects IEC 62443 current parts (2-1, 3-2, 3-3, 4-1, 4-2), NIST CSF 2.0 (February 2024), CERT-In Directions 28 April 2022, DPDP Act 2023 with DPDP Rules notified 13 November 2025, TISAX/VDA ISA current release, Schedule M revised 2024 for pharmaceutical manufacturing, and Cisco Industrial Threat Defense architecture (Cyber Vision).

Written by **Kunal Hans, CTO**

Proactive Data Systems Manufacturing Practice. 25 years designing OT/IT segmentation for automotive, pharma, discrete manufacturing, and process industries across India.

Proactive Data Systems Manufacturing Practice

Cisco Preferred Partner across Networking, Security, Collaboration, Data Center, and Services · Cisco Advanced Customer Experience Specialised · Since 1991.

Preface

Every Indian manufacturing CIO now runs at least three simultaneous programmes: a ransomware defence programme driven by board-level pressure, a Schedule M, TISAX, or ISO 27001 compliance programme driven by customer or regulator demand, and a Make in India / PLI-scheme capacity expansion where the greenfield line must ship products in eighteen months. All three land on the OT/IT boundary. All three break when the boundary is undefined.

This field guide is written for the CIO, Plant IT Head, or Chief Information Security Officer who is planning an OT/IT segmentation programme, retrofitting security into a running plant, expanding into a new facility, or preparing for a TISAX or Schedule M audit. It covers what OT/IT segmentation means in practice, the Purdue Enterprise Reference Architecture and why it still matters, the parts of IEC 62443 that Indian manufacturers actually get audited against, a reference architecture built on Cisco Industrial Threat Defense components, legacy OT protection where you cannot replace a Windows XP HMI, multi-vendor plant floor coordination across Rockwell, Siemens, Schneider, ABB, Honeywell, Emerson, and Yokogawa estates, ransomware defence at the OT boundary, a realistic implementation timeline, cost bands calibrated to Indian market pricing, and the evidence Schedule M and TISAX auditors expect.

The Proactive Data Systems Manufacturing Practice produces it from live OT/IT segmentation programmes at automotive tier-one suppliers, pharmaceutical manufacturers, discrete manufacturers, process industries, and Make-in-India greenfield facilities across India. It is deliberately opinionated on the Purdue Level 3.5 DMZ, current on IEC 62443 revisions, honest on budget, and free of vendor sales language beyond what the architecture requires. Consult your CISO, your OT operations lead, your quality head, and your Schedule M or TISAX coordinator before acting on any specific design decision.

Key Terms

OT (Operational Technology).

Hardware and software that detects or causes a change through direct monitoring or control of physical devices, processes, and events. On a manufacturing floor: PLCs, DCS, SCADA, HMIs, historians, and safety instrumented systems.

IT (Information Technology).

Corporate networks, ERP, MES at the business layer, email, endpoint compute. The systems that stop the business if they go down but do not stop the physical process.

Purdue Model / PERA.

Purdue Enterprise Reference Architecture — a hierarchical model that separates manufacturing operations into levels 0 (physical process) through 5 (enterprise business systems), with Level 3.5 designated as the DMZ between OT and IT. ISA-95 formalises the model in the international standard.

IEC 62443.

The international series of standards for industrial automation and control systems security, published jointly by IEC and ISA. Key parts referenced in this guide: 2-1 (security programme requirements for asset owners), 3-2 (risk assessment for system design), 3-3 (system security requirements and security levels), 4-1 (secure product development lifecycle), 4-2 (technical security requirements for components).

Security Level (SL).

IEC 62443's four-tier classification of the required strength of security controls (SL1 through SL4), from protection against casual or coincidental violation up to protection against intentional violation using sophisticated means with extended resources.

Zone and Conduit.

IEC 62443's method for logically grouping OT assets with common security requirements (a zone) and defining the controlled communication path between zones (a conduit).

DMZ (Demilitarised Zone).

The Purdue Level 3.5 buffer network that mediates all traffic between the Level 4/5 IT enterprise environment and the Level 0-3 OT environment.

Historian.

A time-series database that captures process data from OT systems for engineering analysis, quality, and compliance. AVEVA PI System (formerly OSIsoft PI) is the dominant enterprise-scale platform.

HMI.

Human-Machine Interface — the operator-facing display used to view and interact with the industrial process.

PLC / DCS.

Programmable Logic Controller / Distributed Control System — the control-layer systems that execute the industrial process logic.

Cisco Cyber Vision.

Cisco's OT asset visibility, threat detection, and vulnerability management platform, sold as part of the Cisco Industrial Threat Defense architecture.

TISAX.

Trusted Information Security Assessment Exchange — the assessment and exchange mechanism operated by ENX Association for automotive-industry information security, based on the VDA ISA catalogue.

In Brief

What Proactive Delivers for Manufacturing OT/IT Segmentation:

Purdue-model reference architecture aligned to IEC 62443-2-1, 3-2, 3-3, 4-1, and 4-2. Level 3.5 DMZ design with strict conduit definitions. Cisco Industrial Threat Defense implementation including Cisco Cyber Vision for OT asset visibility and threat detection, Cisco Industrial Ethernet 3200/3300/3400/9300 series switches, Cisco IW-9165/9167 industrial wireless with URWB (Ultra-Reliable Wireless Backhaul), Cisco Secure Firewall for zone-to-zone conduit enforcement, and Cisco Identity Services Engine for OT-aware access control.

Multi-vendor plant floor coordination across Rockwell Automation (Allen-Bradley, ControlLogix, FactoryTalk), Siemens (SIMATIC, TIA Portal), Schneider Electric (Modicon, EcoStruxure), ABB, Honeywell Experion, Emerson DeltaV, Yokogawa Centum, and AVEVA PI System historian estates. Legacy OT protection where Windows XP HMIs and unpatched PLCs cannot be replaced. Ransomware containment architecture with proven blast-radius bounds. Schedule M (pharma), TISAX (automotive), ISO 27001:2022, ISO 22301:2019, and CERT-In evidence packs. Indian market cost bands. The Proactive OT/IT Segmentation Reference Architecture is available as a free download.

Who this is for:

CIOs, CTOs, Plant IT Heads, Chief Information Security Officers, and OT Operations Leads at automotive tier-one and tier-two suppliers, pharmaceutical manufacturers, discrete manufacturers (engineering, electronics, capital goods), process industries (chemicals, cement, steel, oil and gas), and Make-in-India / PLI-scheme greenfield operators in India.

Since:

1991. Proactive Data Systems is a Cisco Preferred Partner across five portfolios and Cisco Advanced Customer Experience Specialised.

What Does OT/IT Segmentation Actually Mean?

OT/IT segmentation means engineering a controlled boundary between the Operational Technology environment (PLCs, DCS, SCADA, HMIs, safety instrumented systems that control the physical manufacturing process) and the Information Technology environment (corporate networks, ERP, email, endpoint compute), such that no traffic crosses the boundary except through explicitly defined, monitored, and enforced conduits. Segmentation is not a VLAN and a firewall rule. It is an architecture that survives a ransomware event on the IT side without stopping the plant, and an OT event without exposing corporate systems.

Three misconceptions dominate the market, and each is worth naming:

- **Segmentation is not just a firewall between IT and OT.**

  A single firewall with permissive rules ("allow ERP-to-MES", "allow historian-to-BI") is not segmentation; it is a router with rules. Proper segmentation implements the Purdue Level 3.5 DMZ with explicit inbound and outbound conduits, an intermediary system for every data flow, and no direct L4/5 to L2/3 communication.

- **Segmentation is not something you install and finish.**

  It is a running architecture with continuous asset discovery (Cisco Cyber Vision), continuous vulnerability tracking, quarterly conduit review, and an incident-response playbook that keeps the plant running when the IT side is compromised.

- **Segmentation is not the OT team's problem or the IT team's problem.**

  It is a joint operating discipline. Plants that treat it as an IT initiative build architectures that operations rejects at the first production disruption. Plants that treat it as an OT initiative build architectures that IT cannot maintain.

What Is the Purdue Model and Why Does It Still Matter?

The Purdue Enterprise Reference Architecture (PERA), formalised in ISA-95, defines hierarchical levels for manufacturing operations:

- Level 0 (physical process: sensors, actuators, motors)
- Level 1 (basic control: PLCs, RTUs, safety instrumented systems)
- Level 2 (area supervisory control: HMIs, SCADA, engineering workstations)
- Level 3 and 3.5 (site manufacturing operations: MES, historians, batch management), and (the DMZ)
- Level 4 (site business planning: ERP, site email, planning)
- Level 5 (enterprise: corporate WAN, corporate ERP, cloud).

It matters because every IEC 62443, TISAX, and Schedule M assessment maps controls to it, and because the Level 3.5 DMZ is where segmentation architectures succeed or fail.

The levels at a glance:

Level	What Lives Here	Typical Devices	Typical Devices
5	Enterprise	Corporate ERP, cloud, corporate WAN	SAP, Oracle, AWS, Azure
4	Site Business	Site ERP, site email, planning	SAP, Oracle
3.5	DMZ	Jump hosts, patch server, anti-virus relay, reverse proxies, replicated historian	Cisco, Fortinet, Palo Alto
3	Site manufacturing operations	MES, batch management, historian primary	AVEVA PI, Wonderware, Rockwell FactoryTalk, Siemens Opcenter
2	Area supervisory	HMIs, SCADA, engineering workstations	Wonderware, Rockwell FactoryTalk View, Siemens WinCC, ABB 800xA
1	Basic Control	PLCs, RTUs, safety instrumented systems	Rockwell ControlLogix, Siemens SIMATIC S7, Schneider Modicon, ABB AC800M, Emerson DeltaV, Honeywell Experion, Yokogawa Centum
0	Physical Process	Sensors, actuators, motors, valves	Sensor and actuator OEMs

Two rules define the Purdue architecture and every practical segmentation design:

- **No direct communication between Level 4/5 and Level 0-3.** Every conversation is mediated through Level 3.5. An ERP that reads production status from a historian talks to a replicated read-only historian in the DMZ, not to the production historian in Level 3.
- **No inbound conduit from IT to OT without a specific, documented, auditable purpose.** Every conduit from L4/5 into L3.5 or below is enumerated, risk-assessed, monitored, and reviewed quarterly. The default answer to "can we add a rule for X" is no.

The Purdue model is thirty-plus years old and continues to hold because the physics of manufacturing has not changed. Cloud, IIoT, and Industry 4.0 add new patterns above and beside the model; they do not replace it. The correct pattern for cloud integration is not "punch a hole from AWS to the PLC"; it is "the PLC data flows through the historian in Level 3, is replicated read-only into Level 3.5, and is pulled from Level 3.5 by the cloud."

What Does IEC 62443 Actually Require?

IEC 62443 is the international standard series for industrial automation and control systems security, jointly developed by IEC and ISA. Indian manufacturers get audited against five parts in particular: 62443-2-1 (security programme requirements for asset owners), 62443-3-2 (risk assessment and system design), 62443-3-3 (system security requirements and security levels), 62443-4-1 (secure product development lifecycle for suppliers), and 62443-4-2 (technical security requirements for components).

What each part actually asks for:

- **IEC 62443-2-1** is about the asset owner's cyber security management system. Governance structure, roles and responsibilities, risk management processes, incident response, business continuity, personnel security, physical security, and management of change. If your OT security programme does not have a documented CSMS, 2-1 is where the auditor starts.
- **IEC 62443-3-2** is about zone and conduit design. Every OT asset lives in a zone with a defined Security Level Target (SL-T). Every communication between zones is a conduit with its own SL-T. Risk assessments justify the SL-T assignments. This is the part of the standard that operationalises Purdue: zones are approximately Purdue levels, conduits are approximately the paths between them.

- **IEC 62443-3-3** defines the seven Foundational Requirements (identification and authentication, use control, system integrity, data confidentiality, restricted data flow, timely response to events, resource availability) and the four Security Levels (SL1 through SL4). A zone's SL-T is achieved when every foundational requirement is met to the assigned level.
- **IEC 62443-4-1** is about the product supplier's secure development lifecycle. Relevant when procuring OT equipment: does the PLC vendor have documented secure development practices?
- **IEC 62443-4-2** is the component-level counterpart to 3-3: the technical security requirements that a single component (PLC, HMI, switch) must meet to be assigned an SL.
- For most Indian manufacturers, 2-1 and 3-3 are where audits start. 3-2 is the design discipline that makes 3-3 achievable. 4-1 and 4-2 shape procurement, not deployment.
- **NIST CSF 2.0 (February 2024) is a complementary framework,** not a replacement. Where IEC 62443 gives you technical detail, NIST CSF 2.0 gives you a governance and outcomes vocabulary that boards and non-technical stakeholders read more fluently. Most mature Indian OT security programmes use both.

What Is the OT/IT Segmentation Reference Architecture?

The reference architecture layers three functional planes across the Purdue model: a network plane (industrial Ethernet, industrial wireless, DMZ firewalls), a visibility and detection plane (Cisco Cyber Vision for OT asset discovery, protocol dissection, and anomaly detection), and an identity and access plane (Cisco Identity Services Engine for OT-aware authentication and posture assessment, with Cisco Secure Firewall enforcing zone-to-zone policy).

The reference build using Cisco Industrial Threat Defense components:

Level 0-1 (physical process, basic control) network layer. Industrial Ethernet switches rated for the plant environment - Cisco IE-3200 for basic hardened switching, IE-3300 for larger port counts and Layer 3 capability, IE-3400 for advanced application hosting and edge compute, IE-9300 for aggregation. Where wired connectivity is impractical (mobile assets, cranes, AGVs, outdoor process areas), Cisco IW-9165 or IW-9167 industrial wireless with URWB for deterministic wireless.

Level 2 (area supervisory) network layer. Ruggedised switching consolidating HMIs, SCADA servers, and engineering workstations. Zoning of each production area or line as an IEC 62443 zone with its own SL-T. Inter-zone conduits enforced through a Cisco Secure Firewall or a Cisco Catalyst switch with strict ACLs.

Level 3 (site manufacturing operations) network layer. MES servers, batch management, primary historian (AVEVA PI Server), and site operations tooling on a dedicated zone with role-based access control through Cisco ISE.

Level 3.5 (DMZ) — the architecture's centre of gravity. Cisco Secure Firewall pair (active-active) enforcing every inbound and outbound conduit. Replicated read-only historian for enterprise consumption. Jump hosts for remote support and vendor access, integrated with Cisco Duo for MFA. Patch server for OT patches. Anti-virus relay for OT-safe signature updates. Reverse proxy for any authorised inbound access. No direct L4/5-to-L2/3 traffic; every conversation is mediated here.

Level 4-5 (site business and enterprise) network layer. Site ERP, corporate WAN, and cloud connectivity through the Cisco Secure Firewall pair with strict conduit definitions to the DMZ. Cisco SD-WAN or SASE for cloud integration.

Visibility plane. Cisco Cyber Vision sensors deployed as software on Cisco IE-3400 or IE-9300 switches (embedded sensor) or as hardware sensors at aggregation points. Cyber Vision Center for asset inventory, vulnerability tracking, communication baselining, and threat detection. Integration with Cisco XDR and the plant's SIEM for centralised alerting.

Identity plane. Cisco ISE for network access control, integrated with Active Directory for IT users and with a dedicated OT identity store for OT users. Certificate-based authentication for engineering workstations and jump hosts. Cisco Duo for MFA on all administrative access to OT systems.

Remote access. No direct RDP or VPN from IT to OT. All remote access is through Level 3.5 jump hosts, session-recorded, MFA-enforced, and time-bounded. Vendor remote access is a specific pattern — per-vendor jump host, per-session approval workflow, session recording retained for the period the audit framework requires.

How Do You Protect Legacy OT Systems You Cannot Replace?

Legacy OT protection is compensating-controls engineering: you cannot patch the Windows XP HMI or replace the twenty-year-old PLC, so you engineer the surrounding environment to make an attack on it hard, contained, and detectable. Five compensating-control patterns cover the majority of real-world Indian manufacturing legacy estates.

Aggressive micro-segmentation. The legacy device sits in its own IEC 62443 zone with the tightest possible conduit set. If a Windows XP HMI needs to talk to one PLC and one historian and nothing else, the network enforces that at the switch or firewall.

Network-based protocol inspection. Cisco Cyber Vision performs deep packet inspection of industrial protocols (Modbus, EtherNet/IP, PROFINET, OPC UA, DNP3, IEC 61850) and flags anomalous traffic. Behavioural baselines are established during a discovery period; deviations trigger alerts.

Application whitelisting on the endpoint. Where the legacy Windows system permits agent installation, application whitelisting (Cisco Secure Endpoint or equivalent) prevents unauthorised binaries from executing. Where it does not, the network layer bears the load.

Restricted physical access. USB ports disabled or physically sealed. Local console access controlled. Removable media policy enforced through OT-safe patrol.

Bounded blast radius. If the legacy device is compromised, the network layer prevents lateral movement. This is the payoff of proper zone and conduit design: a compromised HMI can only reach what the conduits allow it to reach, which is a very short list.

These patterns are not perfect. They are what makes the compliance and risk position defensible while the legacy replacement programme runs in parallel over three to seven years, aligned to plant capacity refresh cycles.

How Do You Handle Multi-Vendor OT Environments?

Multi-vendor OT environments are the norm across Indian manufacturing, particularly in automotive, pharma, and process industries where plant expansions and acquisitions have layered vendor estates on top of each other. The reference architecture handles them by treating each vendor's control system as a set of IEC 62443 zones with vendor-specific engineering support paths, standardising the network and DMZ layers underneath, and coordinating change management across the OT engineering teams that operate each estate.

Practical patterns for the vendor stacks Indian manufacturers actually run:

- **Rockwell Automation** (Allen-Bradley PLCs, ControlLogix, CompactLogix, FactoryTalk SCADA and MES): CIP-Security-aware Ethernet/IP switching. FactoryTalk AssetCentre integration for change management. Cisco Cyber Vision supports Rockwell protocol dissection.

- **Siemens** (SIMATIC S7 PLCs, WinCC, TIA Portal, SIMATIC PCS 7 DCS, Opcenter MES): PROFINET-aware switching. TIA Portal integration for engineering workflows. Cisco Cyber Vision supports PROFINET dissection.
- **Schneider Electric** (Modicon PLCs, EcoStruxure, Foxboro I/A Series DCS): Modbus TCP and Ethernet/IP-aware switching. Cisco Cyber Vision supports Modbus dissection.
- **ABB** (AC800M PLCs, 800xA DCS, AbilityEdge): PROFIBUS and Ethernet-based control. Cisco Cyber Vision supports ABB traffic patterns.
- **Honeywell** (Experion PKS DCS, ControlEdge PLCs): Honeywell-specific protocol support. Managed DMZ integration for Honeywell Trace and other Honeywell tools.
- **Emerson** (DeltaV DCS, Ovation): Emerson-specific engineering workflows. Segmented conduit for DeltaV workstations.
- **Yokogawa** (Centum VP DCS, ProSafe-RS SIS): Yokogawa-specific control network. Careful conduit design around safety instrumented systems.
- **Historian layer.** AVEVA PI System (formerly OSIsoft PI, following AVEVA's acquisition of OSIsoft in 2021) is the dominant enterprise historian; the reference architecture places the primary PI Server in Level 3 with a replicated read-only PI in Level 3.5 for enterprise and cloud consumption. GE Digital Historian (Proficy), Rockwell FactoryTalk Historian, and Wonderware Historian follow the same pattern where deployed.

The key architectural discipline: the network, DMZ, and identity layers are standardised across vendors. What varies is the engineering-support conduit pattern into each vendor's control estate.

How Do You Defend Against Ransomware in OT?

Ransomware defence in OT is architected around three outcomes: preventing the initial compromise from reaching OT in the first place (containment at Level 3.5), detecting the compromise fast enough to isolate before it spreads (Cisco Cyber Vision and Cisco XDR), and recovering the OT environment even when the IT environment is unrecoverable (OT-native backups, air-gapped copies, and a tested recovery playbook).

Six architectural elements form the OT ransomware defence stack:

Segmentation as the first line. Ransomware that lands on the corporate network via phishing or a compromised vendor endpoint stops at Level 3.5 because there is no direct path to Level 2 or Level 1. The Colonial Pipeline (US, 2021), Norsk Hydro (Norway, 2019), and multiple Indian manufacturing incidents in FY24 all shared a preventable-with-segmentation failure mode.

OT-aware detection. Cisco Cyber Vision baselines normal OT communication and alerts on new device appearances, new protocol conversations, or industrial protocol commands that should not exist (write commands from an HMI that has never issued them, firmware update sequences to a PLC outside a change window).

Immutable and air-gapped backups. OT configuration backups (PLC programs, HMI configurations, DCS project files, batch recipes, historian data) held in immutable storage with an air-gapped copy. Backup validation on a scheduled cadence.

Recovery playbook tested twice a year. Not a document. A drill. Time from "we are compromised" to "line X is producing again" is a measured metric, not an assumption.

IT ransomware event does not stop the plant. The plant runs autonomously through the event. Order flow, ERP integration, and MES batching may be manual for the recovery window, but the physical process continues. This is the design goal that separates a mature OT security posture from an IT-security-programme-with-OT-bolted-on.

Insurance and reporting readiness. Cyber insurance policies for Indian manufacturers now routinely require evidence of IEC 62443-aligned segmentation, tested recovery playbooks, and quarterly Cyber Vision reports. CERT-In notification (six hours from awareness) is a legal requirement under the CERT-In Directions of 28 April 2022.

For manufacturers whose facilities are notified as Critical Information Infrastructure (defence, aerospace, energy-adjacent, semiconductor fabrication under India's Semiconductor Mission), additional obligations under the National Critical Information Infrastructure Protection Centre (NCIIPC) framework apply and are worth engaging with directly.

What Does an OT/IT Segmentation Programme Cost in India?

An OT/IT segmentation programme for an Indian manufacturing site typically lands in one of three budget bands, driven by plant size (network drops and OT device count), vendor mix complexity, legacy density, and whether the site is retrofit or greenfield. The figures below are indicative Indian-market bands at August 2026 and should be treated as planning anchors, not quotations.

Per-site cost bands (retrofit of an existing single-site plant):

Per-site cost bands (retrofit of an existing single-site plant):

Site Profile	Typical Scope	Programme Cost Band (INR)
Small plant (50-150 OT devices, single vendor, single line)	Purdue L3.5 DMZ, single-zone L2, Cyber Vision entry deployment, IEC 62443-3-3 SL1 target	₹1.2 crore – ₹2.5 crore
Mid-size plant (150-500 OT devices, 2-3 vendors, 3-8 lines)	Full Purdue architecture, multi-zone L2, Cyber Vision full deployment, IEC 62443-3-3 SL2 target, ISE integration	₹3 crore – ₹6 crore
Large plant (500-2,000 OT devices, 4+ vendors, complex process)	Full Purdue with process-specific SIS zoning, complete visibility and identity plane, IEC 62443-3-3 SL2-SL3 target, TISAX or Schedule M evidence pack	₹6 crore – ₹15 crore
Multi-plant enterprise programme (5-plus sites, common architecture)	Reference architecture template, per-plant customisation, central Cyber Vision Center, enterprise-scale SIEM integration	₹18 crore – ₹60 crore across 24-36 months

Bands include: network hardware (industrial switches, wireless, aggregation), DMZ firewalls and jump hosts, Cyber Vision sensors and Center, ISE and Duo, first-year support, professional services (design, deployment, integration, evidence generation), and change management for OT operations teams. Bands exclude: OT device replacement (which is a capital programme in its own right), plant downtime opportunity cost, and any application-layer work on MES, ERP, or historian.

For greenfield Make-in-India / PLI-scheme facilities, the correct comparison is not "cost of segmentation retrofit" but "incremental cost over an unsegmented greenfield build" - typically 8-15% of total plant IT and OT network capex, which is materially cheaper than any retrofit for the same architectural outcome.

Regional variation and volume-driven negotiation can shift the bands 15-25%. Programmes that use existing OT team hours for change management and validation land at the lower end; programmes that require Proactive to backfill OT operations bandwidth land at the higher end.

What is a Realistic Implementation Timeline?

A realistic OT/IT segmentation programme for a mid-size Indian manufacturing site takes 9 to 15 months from initial risk assessment through validated cutover, driven by plant change-window availability rather than engineering effort. Greenfield sites integrate segmentation into commissioning at no additional programme time. Multi-site enterprise programmes run 24 to 36 months across a phased site rollout.

The five phases:

Phase 1: Discovery and assessment (weeks 1-8). Cisco Cyber Vision deployed in passive listening mode to build the OT asset inventory. Interviews with OT operations, quality, and IT teams. IEC 62443-3-2 risk assessment. Baseline of current communication patterns. Deliverable: zone and conduit design proposal aligned to plant reality.

Phase 2: Reference architecture design (weeks 6-12). Purdue L3.5 DMZ design. Zone and conduit specification. SL-T assignments per IEC 62443-3-3. Change management plan aligned to plant production calendar. Deliverable: architecture document and staged migration plan.

Phase 3: Non-disruptive foundation (weeks 10-24). DMZ deployment, ISE deployment, Cyber Vision Center hardening, jump host and MFA build-out. All work non-disruptive to production. Deliverable: L3.5 operational and instrumented.

Phase 4: Zone-by-zone migration (weeks 20-44). Each production zone migrated to its target architecture during planned maintenance windows or plant shutdowns. Testing before, during, and after each cutover. Deliverable: each zone in compliance with its SL-T, with evidence pack captured.

Phase 5: Validation, evidence, and handover (weeks 40-52). Full penetration test aligned to IEC 62443 threat model. TISAX, Schedule M, ISO 27001, or CERT-In evidence pack finalised. Handover to plant IT and OT operations teams with runbook. Deliverable: audit-ready site. The dominant constraint is the plant's production calendar. Automotive plants with 24/7 line operations get 4-8 hour change windows every fortnight and full-day shutdowns quarterly. Pharma plants get change windows aligned to campaign changeovers. Continuous-process plants (steel, cement, chemicals) get windows during scheduled turnarounds only. Design must respect this or the programme stalls.

What Schedule M, TISAX, ISO 27001, and CERT-In Evidence Do You Need?

Schedule M (pharmaceutical manufacturers), TISAX (automotive supply chain), ISO 27001:2022 (general information security), ISO 22301:2019 (business continuity), and CERT-In Directions (all Indian entities) each look at OT security through their own lens. The evidence patterns overlap substantially, and a well-designed segmentation programme produces evidence that satisfies most or all frameworks simultaneously.

Schedule M evidence (pharmaceutical manufacturers only). Schedule M under the Drugs and Cosmetics Rules was revised and notified in December 2023 with phased effective dates through 2024-2025 for different manufacturer sizes. It requires computerised systems validation (CSV) aligned to GAMP 5 principles, data integrity controls under ALCOA+ principles, and Part 11-equivalent audit trails for GxP-relevant computerised systems.

Segmentation evidence includes: documented Purdue architecture with GxP systems zoned; access control to GxP systems with role-based approval workflow; audit trail configurations; change management records for every GxP system change. Only pharma manufacturers are subject to Schedule M; the framework does not apply to automotive, engineering, or other manufacturing sectors.

TISAX evidence (automotive supply chain). TISAX is based on the VDA ISA (Verband der Automobilindustrie Information Security Assessment) catalogue and is required by most global automotive OEMs for their suppliers. Evidence includes: IEC 62443-aligned zone and conduit design, personnel security records, physical security records, incident response records, business continuity records, and specific prototype protection controls for suppliers handling pre-production designs. TISAX assessment levels (AL 1, 2, 3) determine the depth of assessment.

ISO 27001:2022 evidence. The 2022 revision restructured Annex A controls into four themes (organisational, people, physical, technological). OT/IT segmentation evidence maps predominantly to organisational (governance, third-party) and technological (network security, secure configuration, secure development) themes. A well-run segmentation programme produces evidence that supports 40 to 60% of the technological Annex A controls directly.

ISO 22301:2019 evidence (business continuity). OT/IT segmentation is a business continuity control: the plant continues to run when IT is compromised. ISO 22301 evidence includes the tested recovery playbook, RTO/RPO commitments per business process, and validated backup and restoration cadence.

CERT-In evidence. CERT-In Directions of 28 April 2022 apply to all Indian entities including manufacturers. Six-hour incident notification workflow, 180-day log retention within India, mandatory NTP synchronisation to NIC or NPL time sources, and specific KYC and log retention requirements. Evidence includes the incident response runbook, SIEM ingestion inventory covering OT and IT, and any past incident notification records within the assessment period.

DPDP evidence. DPDP Act 2023 with DPDP Rules notified 13 November 2025 applies where the manufacturer processes personal data - employee data, customer data, and, for consumer product manufacturers, end-customer data. Segmentation supports DPDP by containing exposure of personal data stores. Full DPDP evidence extends beyond segmentation into consent management, DPO structure, and data subject request handling.

NCIIPC obligations (Critical Information Infrastructure). Manufacturers whose facilities are notified as CII (defence, aerospace, energy-adjacent, and increasingly semiconductor fabrication under the India Semiconductor Mission) have additional NCIIPC obligations that operate alongside the frameworks above.

What Are the Common Mistakes in Indian Manufacturing OT/IT Segmentation?

The nine most common mistakes across Proactive's Indian manufacturing engagements in the last four quarters cluster in scope, ownership, design assumptions, and post-cutover discipline. Eight are engineering or change-management issues that a properly scoped programme designs out. One is structural and worth naming honestly.

Treating segmentation as an IT initiative. OT operations is not represented in the design phase. The architecture is technically correct and operationally unusable. The plant rejects it at the first cutover attempt.

Skipping the discovery phase. TProgramme starts with a firewall procurement decision. The team learns during deployment that the actual OT asset inventory is 40% larger than documented and includes vendors and protocols nobody knew about.

Level 3.5 DMZ implemented as a routed VLAN. No real conduit enforcement, no intermediate systems, no MFA on jump hosts. The DMZ exists on the network diagram and not in the traffic path.

Ignoring vendor engineering support paths. The architecture cuts off Rockwell or Siemens engineering support from remote diagnosis. When a production issue occurs, operations demands "just open the port", and the segmentation is undermined within the first quarter.

No baseline of normal OT communication before cutover. Post-cutover, every change looks like an anomaly. Alert fatigue sets in. Cyber Vision alerts get ignored.

Backups untested. The recovery playbook exists in a document. Nobody has ever actually restored a PLC configuration or a historian data set from backup. When a ransomware event happens, the recovery time surprises everyone unpleasantly.

Change management not aligned to plant production calendar. Cutover attempted during production hours. The programme is postponed, the OT team loses trust, and the residual cutovers slip by quarters.

No handover to operations. Programme ships an architecture nobody in the plant knows how to run. Six months later, the environment has drifted from the reference architecture and the evidence pack is stale.

Structurally hard, worth naming: OT team hiring is a national bottleneck. Indian manufacturing struggles to recruit OT security engineers with both control-system fluency (PLC programming, DCS operations, SIS understanding) and network-security depth (IEC 62443, Cisco Cyber Vision, firewall policy). The talent pool is measurable in low four-digit numbers nationally, concentrated in a handful of Tier-1 metros and industrial belts (Pune, Chennai, Ahmedabad, Delhi NCR). This is not a problem a segmentation programme can solve; it is a structural constraint the CIO plans around by combining internal upskilling, partner-provided managed services (Proactive included), and vendor education investment over three-year horizons.

Frequently Asked Questions

What is OT/IT segmentation and why does Indian manufacturing need it?

OT/IT segmentation is the engineered boundary between manufacturing control systems (PLCs, DCS, SCADA, HMIs) and corporate IT (ERP, email, corporate WAN), implemented through the Purdue Level 3.5 DMZ with explicit zones, conduits, and mediated data flows. Indian manufacturers need it for ransomware defence, TISAX and Schedule M compliance, ISO 27001:2022 alignment, CERT-In compliance, and, for critical infrastructure manufacturers, NCIIPC obligations.

What does IEC 62443 require in practice?

Five parts matter for Indian manufacturers: 62443-2-1 (cyber security management system), 62443-3-2 (zone and conduit design and risk assessment), 62443-3-3 (seven Foundational Requirements and four Security Levels), 62443-4-1 (product supplier secure development), and 62443-4-2 (component technical requirements). 2-1 and 3-3 are where most Indian manufacturing audits start; 3-2 is the design discipline that makes 3-3 achievable.

How does Proactive design OT/IT segmentation across multi-vendor plant floors?

The network, DMZ, and identity layers are standardised across vendors using Cisco Industrial Threat Defense components. Vendor-specific engineering-support conduits are designed per vendor estate - Rockwell, Siemens, Schneider, ABB, Honeywell, Emerson, Yokogawa - with protocol-aware visibility from Cisco Cyber Vision. AVEVA PI System (formerly OSIsoft PI) historian layer is standardised across the multi-vendor floor.

How do you protect legacy OT you cannot replace?

Five compensating-control patterns: aggressive micro-segmentation placing the legacy device in its own IEC 62443 zone; network-based protocol inspection using Cisco Cyber Vision; application whitelisting on the endpoint where the OS permits it; restricted physical access with disabled USB and controlled console access; and bounded blast radius through strict conduit design. Legacy replacement runs in parallel over three to seven years, aligned to plant capacity refresh.

What's the typical timelHow long does an OT/IT segmentation programme take at an Indian manufacturing site?ine for a hospital Wi-Fi refresh?

A 400-bed tertiary care hospital typically runs 90 to 150 days from kickoff to steady state, phased around the clinical calendA mid-size Indian manufacturing site typically takes 9 to 15 months from initial risk assessment through validated cutover, driven by plant change-window availability. Greenfield Make-in-India facilities integrate segmentation into commissioning at no additional programme time. Multi-site enterprise programmes run 24 to 36 months across a phased rollout.ar. Multi-facility hospital chains typically start with a foundational programme at one flagship facility (90 days) and roll out to subsequent facilities on 60-day cycles per facility.

What does an OT/IT segmentation programme cost in India?

Per-site bands (August 2026 planning anchors): ₹1.2-₹2.5 crore for a small plant (50-150 OT devices); ₹3-₹6 crore for a mid-size plant (150-500 OT devices); ₹6-₹15 crore for a large plant (500-2,000 OT devices). Multi-plant enterprise programmes land at ₹18-₹60 crore across 24-36 months. For greenfield builds, segmentation typically adds 8-15% incremental cost over an unsegmented build, materially cheaper than any retrofit.

Does segmentation help against ransomware?

Yes, directly. Ransomware that lands on the corporate network via phishing or a compromised vendor endpoint is contained at Level 3.5 because there is no direct path from IT to OT control systems. Colonial Pipeline (2021), Norsk Hydro (2019), and multiple Indian manufacturing incidents in FY24 shared a preventable-with-segmentation failure mode. Combined with OT-native backups and a tested recovery playbook, segmentation keeps the plant running through an IT ransomware event.

Which manufacturers need Schedule M vs TISAX vs both?

Schedule M applies only to pharmaceutical manufacturers under the Drugs and Cosmetics Rules. TISAX applies to automotive supply chain suppliers where global OEMs mandate it. A manufacturer producing both pharmaceutical and non-pharmaceutical products may need Schedule M for the pharma facility and separate certification (ISO 27001, TISAX, or customer-specific) for the non-pharma facility. ISO 27001:2022 and CERT-In apply to all Indian entities regardless of sector.

Why This Guide, From Proactive

Every Indian manufacturing CIO we work with has the same three-headed pressure: the board wants ransomware defence, the customer or regulator wants TISAX or Schedule M evidence, and the plant wants the segmentation programme to leave production untouched.

The OT team and the IT team disagree on what "left alone" means. Proactive Data Systems has spent the last decade designing OT/IT segmentation where those constituencies meet - across automotive tier-ones and tier-twos, pharmaceutical manufacturers, discrete manufacturers, process industries, and Make-in-India / PLI-scheme greenfield facilities.
We are a Cisco Preferred Partner across five portfolios - Networking, Security, Collaboration, Data Center, and Services - with the Cisco Advanced Customer Experience Specialised designation. Founded in Delhi NCR in 1991. Over 1,500 enterprise customers across India. More than 100 certified engineers.

A dedicated manufacturing practice with implementations across India's major industrial belts, including Chakan-Pune, Chennai-Sriperumbudur, Ahmedabad-Sanand, Delhi NCR-Manesar, and Hyderabad-Vizag.

When Indian manufacturing CIOs ask us to compare our approach to alternatives, a Cisco or Rockwell direct professional services engagement, a global systems integrator programme, or a specialist OT security boutique, three points typically decide the engagement. First, we design the network, visibility, and identity planes as a single integrated architecture, not as three vendor workstreams that later have to be reconciled. Second, we carry Cisco specialisations across the full Industrial Threat Defense portfolio plus current vendor familiarity with the OT ecosystem Indian manufacturing actually runs (Rockwell, Siemens, Schneider, ABB, Honeywell, Emerson, Yokogawa, AVEVA PI System). Third, our implementations produce evidence packs formatted for TISAX assessors, Schedule M inspectors, ISO 27001 auditors, and CERT-In reviewers - not just for the internal IT team.

If you are planning an OT/IT segmentation programme, retrofitting security into a running plant, expanding into a greenfield facility, or preparing for a TISAX or Schedule M audit, book a 30-minute conversation with a Proactive manufacturing infrastructure architect who has delivered OT security at plants that look like yours and can defend the recommendations to your CISO, your Plant Head, and your customer or regulator.

Proactive Data Systems is an enterprise IT infrastructure and services company. For more than three decades, the company has designed, deployed, and operated the technology foundations behind some of India's most demanding enterprise environments, from regulated industries to large distributed operations.

Founded in 1991, Proactive serves more than 1,500 customers, from fast-growing businesses to Fortune 500 enterprises, across banking and financial services, manufacturing, healthcare, public sector, IT and ITES, retail, education, and global capability centres. Our work spans enterprise networking, cybersecurity, cloud and AI-ready data centres, collaboration platforms, structured cabling, and managed services.

A Cisco Preferred Partner under the Cisco 360 Partner Program, Proactive is recognised across the Networking, Security, Collaboration, Cloud & AI, and Services portfolios, and is a Cisco Advanced Customer Experience Specialised Partner. The company is ISO 9001:2015 and ISO/IEC 27001 certified, and engineers solutions in partnership with Dell, Nutanix, NetApp, Palo Alto Networks, Fortinet, VMware, Veeam, and CommScope.

Headquartered in Delhi NCR, with offices in Mumbai, Bengaluru, Pune, Hyderabad, Indore, and Singapore.

To learn more about our solutions, write to us
at pro@proactive.co.in

www.proactive.co.in

PROACTIVE™
Enhancing Digital Experience