

White Paper

MFA for Manufacturing

Securing OT, IT, and the Hybrid Plant in India

A practical guide for plant managers, IT heads, and security leaders navigating identity security across converged industrial environments

Published by Proactive Data Systems Pvt Ltd

Cisco Preferred Partner — Security, Networking, Collaboration, Cloud & AI, and Services
35 years in Indian IT infrastructure | Delhi · Mumbai · Pune · Bengaluru · Hyderabad · Singapore

Contents

MFA for Manufacturing: Securing OT, IT, and the Hybrid Plant in India	3
Section 1: The Identity Problem Indian Manufacturers Have Not Solved	4
Section 2: Why MFA Is Not Optional in Indian Manufacturing	6
Section 3: The OT Authentication Challenge — and How to Solve It	9
Section 4: Designing the Hybrid Plant Identity Architecture	13
Section 5: The Indian Manufacturing Context	15
Section 6: A Phased Deployment Roadmap	18
Section 7: What Good Looks Like — The Target State	22
Section 8: Key Statistics for Indian Manufacturing Security Leaders	23
Conclusion: The Plant That Cannot Be Breached Through a Credential	24

MFA for Manufacturing: Securing OT, IT, and the Hybrid Plant in India

Up Front

Indian manufacturing is the second most attacked industry in the country, absorbing more than 2,100 cyberattacks per organisation per week. The attack vector has changed. It is no longer the perimeter. It is the identity layer — the shared accounts, the unmonitored vendor sessions, the remote engineering access that nobody formally decommissioned when the integrator finished the project eighteen months ago.

This white paper is written for the people who have to fix that: plant IT heads in Pune, security managers at automotive Tier-1s in Chennai, operations directors at pharmaceutical manufacturers in Hyderabad, and the CISO teams running hybrid environments where a 20-year-old SCADA system sits on the same network as a cloud-connected MES.

It covers why identity is the new perimeter in manufacturing, what MFA can and cannot do in an OT environment, how to design an authentication architecture that works across IT and OT without disrupting production, and what a phased deployment looks like for an Indian plant with realistic constraints.

Section 1: The Identity Problem Indian Manufacturers Have Not Solved

1.1 The attack reached manufacturing before manufacturing was ready

India's manufacturing sector did not arrive at its current security exposure gradually. It arrived abruptly, as the convergence of IT and OT — driven by Industry 4.0 adoption, remote monitoring mandates, supply chain digitalisation, and the operational demands of post-pandemic distributed management — connected systems that were never designed to be connected, and left identities that were never designed to be managed.

In 2025, 55% of Indian manufacturers reported multiple security breaches in a single year. Manufacturing accounted for 68% of all ransomware incidents impacting industrial entities globally in Q1 2025 (Dragos Year in Review, 2025). The sector is no longer an incidental target. It is a primary one, and for a specific reason: manufacturing environments carry the highest asymmetry between attack cost and operational impact of any industry. A credential compromise that takes minutes to execute can shut down a production line that costs the organisation far more per hour than the attack itself.

The attacks hitting Indian manufacturers are not primarily technical exploits targeting zero-day vulnerabilities in PLCs. They are credential attacks: stolen passwords, compromised remote access sessions, vendor accounts that remain active long after the vendor engagement ended, shared engineering workstation logins that have never had individual accountability. These are identity failures. They are preventable.

Every identity access decision in a manufacturing environment comes down to four questions: Is this access verified to a named individual? Is the device it comes from in a known, healthy state? Is the access scoped to what is actually needed? And can it be revoked instantly when it is no longer needed? In most Indian manufacturing environments today, the honest answer to most of those questions is no.

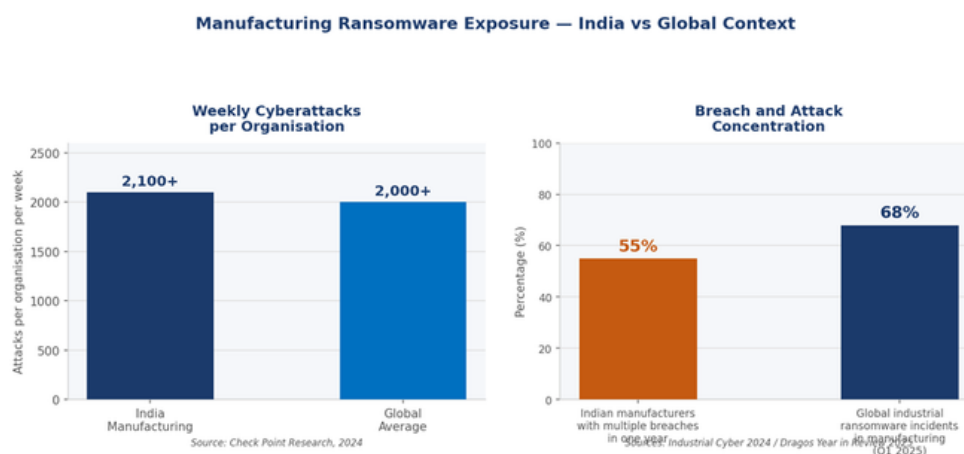


Figure 1: Manufacturing Ransomware Exposure — India vs Global Context (Check Point Research 2024 / Dragos 2025 / Industrial Cyber 2024)

1.2 The shared account problem

Walk into the control room of a mid-sized Indian plant — automotive components in Pune, pharmaceutical production in Hyderabad, FMCG processing in Ahmedabad — and you will find a version of the same thing: a Windows-based HMI or SCADA workstation logged in as "admin," or "operator," or the name of the SCADA platform itself. No individual accountability. No session logging tied to a named user. No MFA. Often, no password policy of any kind.

This is not negligence. It is a practical adaptation to an environment where individual authentication was historically incompatible with operational requirements. Operators rotate across shifts. Production cannot wait for a password reset. The engineering workstation needs to be accessible in an emergency at 2 AM. These constraints are real. They are also solvable — but they require a different approach to MFA architecture than the one that works for an office IT environment.

1.3 The vendor access problem

Third-party vendor access is the largest unmanaged identity risk in Indian manufacturing today. SCADA integrators, PLC programmers, DCS vendors, HVAC contractors, and OEM service teams all require periodic access to OT systems. In practice, this access is typically granted through a shared VPN credential, a shared remote desktop account, or physical on-site access to an unlocked engineering workstation. In most cases, the access is not time-limited, not session-recorded, not scoped to the specific system requiring work, and not formally revoked after the engagement ends.

The attack chain this creates is well-documented: a vendor's laptop is compromised. The attacker uses the vendor's standing remote access credentials to connect to the manufacturer's OT environment. Lateral movement across a flat network reaches critical control systems. The breach is not discovered for weeks, because there are no logs tied to individual sessions. This is the initial access vector in a disproportionate share of industrial cyberattacks globally. Indian manufacturers are not exceptions — they are, in many cases, easier targets because the vendor access governance gap is wider and less acknowledged.

Section 2: Why MFA Is Not Optional in Indian Manufacturing

2.1 The regulatory framework is hardening

Indian manufacturers have historically operated with limited cybersecurity regulation specific to OT environments. That is changing at pace.

The DPDP Act's full substantive compliance deadline of 13 May 2027 requires "reasonable security safeguards" for any organisation processing personal data. This applies to every manufacturer of meaningful scale. In every credible legal reading, reasonable security safeguards in 2026 means MFA is not optional.

CERT-In's mandatory reporting and audit requirements, effective July 2025, require Indian organisations in critical sectors to document access controls and demonstrate incident response capability. Shared accounts and unmanaged vendor access are audit findings.

For manufacturers that are part of global supply chains, IEC 62443 — the international standard for industrial automation and control system security — is an increasingly de facto requirement, enforced through customer contracts and supplier qualification processes. At Security Level 2 and above, IEC 62443 explicitly requires MFA for SCADA servers, management stations, and VPN access. Indian automotive, aerospace, and pharmaceutical manufacturers exporting to global markets are encountering this requirement in tender documents and supplier audits.

Regulation	Effective Date	MFA Implication for Manufacturers
CERT-In Mandatory Audits	July 2025	Document access controls; demonstrate individual accountability for system access; shared accounts are an audit finding
RBI Authentication Directions 2025	1 April 2026	Relevant to BFSI-adjacent manufacturers; mandates flexible 2FA for digital payment transactions
DPDP Act — Full Compliance	13 May 2027	"Reasonable security safeguards" for all personal data processing; MFA is required in all credible legal interpretations
IEC 62443 (de facto)	Supply chain / ongoing	Security Level 2+ mandates MFA for SCADA servers, management stations, VPN access; increasingly enforced through OEM supplier qualification

Table 1: Indian Manufacturing Compliance Calendar — Identity Security Implications



Figure 2: The Indian Manufacturing Compliance Clock — four regulatory deadlines, three already effective

2.2 MFA blocks the attack vector that is actually being used

The case for MFA in manufacturing is not primarily regulatory. It is operational. The credential attacks hitting Indian manufacturers are automated, persistent, and increasingly AI-augmented. Password spraying tools cycle through hundreds of thousands of credential combinations per hour. Infostealer malware — which compromised more than 44,000 Windows systems in India in a three-month period in 2025 — harvests credentials silently and sells them on dark web markets. Attackers purchase those credentials and use them weeks or months later.

MFA does not solve every security problem. It solves the credential problem — the specific vector responsible for the overwhelming majority of initial access in manufacturing breaches. An attacker with a valid username and password, but without the second factor, cannot authenticate. The credential is worthless. Microsoft research shows MFA blocks more than 99% of automated credential attacks. In an environment where credential attacks are the primary initial access vector, that is a fundamental reduction in breach probability — not a marginal improvement.

2.3 The downtime cost: the arithmetic, shown

Indian plant managers are rightly sceptical of security investments that create operational friction. The calculus changes when the cost of a ransomware-driven production shutdown is put on the same scale as the cost of implementing MFA.

According to Comparitech's analysis of 858 confirmed ransomware attacks on manufacturing companies between 2018 and 2024, the average downtime cost in manufacturing is \$1.9 million per day. Manufacturing organisations took an average of 30 days to fully restore operations following a ransomware incident (Sophos State of Ransomware in Manufacturing and Production, 2025). The average recovery cost — excluding any ransom paid — was \$1.3 million (Sophos, 2025). In 2024, 65% of manufacturing organisations globally reported being hit by ransomware.

Apply those figures directionally to an Indian mid-market manufacturer. At \$1.9 million (~₹15.8 crore) per day of downtime, even a four-day partial shutdown — well below the 30-day average — represents roughly ₹63 crore in direct production and recovery exposure before factoring in customer penalties, supply chain disruption costs, and reputational damage with OEM customers.

The total cost of a properly implemented MFA deployment for a 500-user plant environment — licensing, implementation, user enrolment, and helpdesk training — is a fraction of one day of ransomware downtime. This is arithmetic. MFA is not a security cost. It is production insurance.

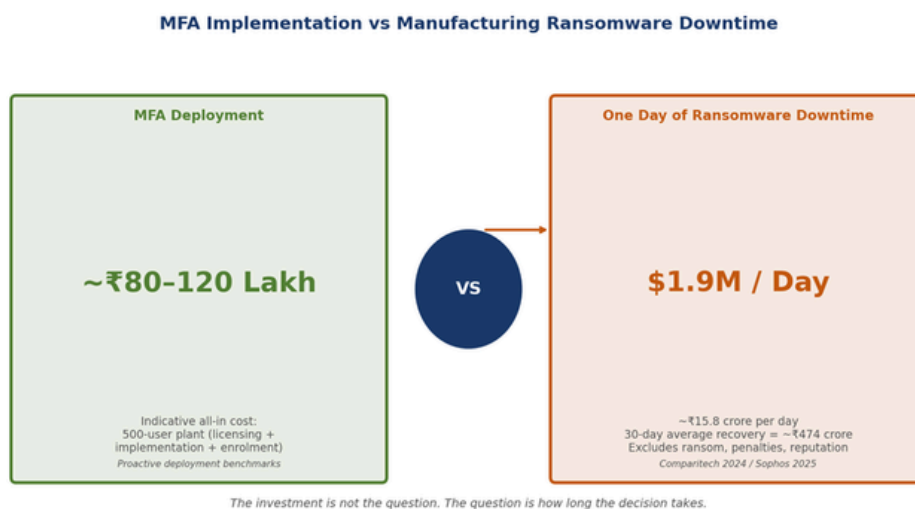


Figure 3: MFA Deployment Cost vs Manufacturing Ransomware Downtime (Comparitech 2024 / Sophos 2025)

Section 3: The OT Authentication Challenge — and How to Solve It

3.1 Why standard IT MFA does not work in OT

The challenge of deploying MFA in an OT environment is not that it cannot be done. It is that applying an IT-designed authentication model directly to OT without adaptation creates operational problems that undermine both security and production continuity. OT environments have characteristics that IT environments do not.

Shared operator roles

Multiple operators work the same HMI or SCADA workstation across shifts. Individual authentication is operationally correct, but the enrolment model must account for shift patterns, shared hardware, and operator rotation.

Legacy protocols and systems

Many SCADA platforms, historians, and DCS controllers running in Indian plants today were designed before modern authentication standards existed. They do not natively support SAML, OAuth, or FIDO2. An authentication proxy — a lightweight server that intercepts the logon request, enforces MFA, and passes through an authenticated session — enables MFA

enforcement without requiring any modification to the legacy application itself.

Latency sensitivity

In a process control environment, authentication delay can be operationally dangerous. An operator responding to an alarm condition cannot wait fifteen seconds for a push notification to approve before taking action. Session-based authentication — where MFA is enforced once at the start of a shift session rather than at every individual application access — is the standard solution for this constraint.

Physical access constraints

Consider where your operators actually work: a press shop floor in Pune where operators wear heavy gloves throughout the shift; a pharmaceutical clean room in Hyderabad where mobile phones are prohibited; a chemical plant in Dahej where only intrinsically safe equipment is permitted; a foundry in Coimbatore where dust and heat make touchscreens unreliable. Smartphone-based push notification — the default factor in most enterprise MFA deployments — does not work in any of these environments. Authentication factors must be selected with the physical reality of the work environment in mind.

Break-glass scenarios

Production emergencies require emergency access capability. Every MFA architecture for OT must include a documented, tested, and audited break-glass procedure. This is not a security exception — it is a required component of responsible OT identity architecture.

3.2 The Purdue Model as the design framework

The Purdue Model provides the architectural foundation for thinking about identity and authentication across a manufacturing environment. MFA policy should be differentiated by zone, not uniform across all levels.

Purdue Level	Systems	MFA Approach	Session Model
Level 0 — Field devices	Sensors, actuators, PLCs (process)	Physical access control only	N/A
Level 1 — Basic control	PLCs, RTUs, safety systems	MFA-enforced remote/vendor access; session recording	Time-limited per engagement
Level 2 — Supervisory	SCADA, DCS, HMI	Authentication proxy for legacy; hardware tokens for operators	Shift-based session
Level 3 — Site operations	Historian, MES, plant-level network	AD-integrated MFA; device health checks	Standard session + idle timeout
Level 4/5 — Enterprise	ERP, business applications, cloud	Full adaptive MFA; push notification or TOTP	Standard enterprise policy

Table 2: Authentication Architecture by Purdue Level — MFA approach differentiated by zone

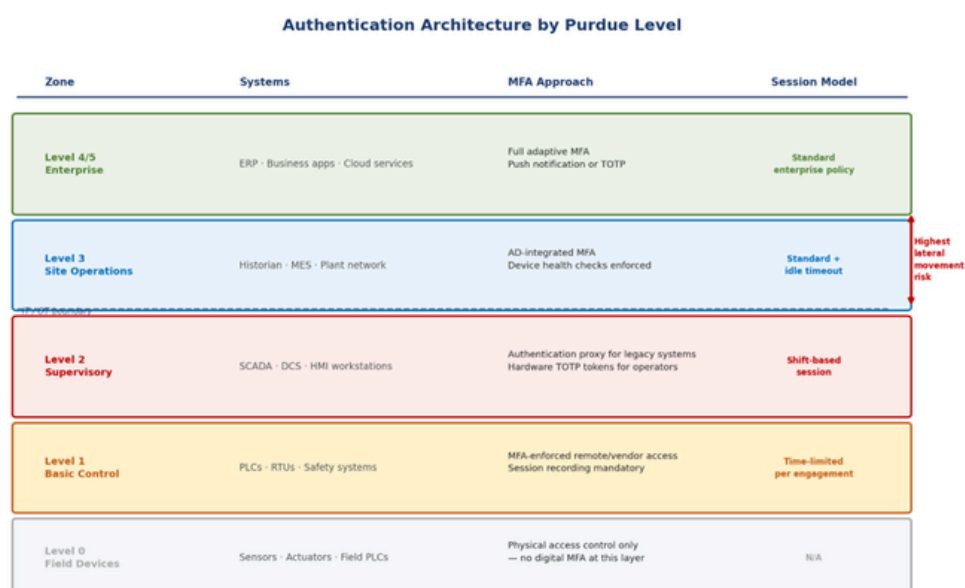


Figure 4: Authentication Architecture by Purdue Level — MFA approach differentiated by zone

3.3 Practical MFA approaches by zone

Level 2 — SCADA and HMI (the hardest problem)

Deploy an authentication proxy between the operator workstation and the SCADA platform. This enables MFA enforcement without requiring the SCADA platform to be modified — critical for legacy systems running on proprietary protocols that cannot be touched without vendor certification. Cisco Duo's Authentication Proxy supports this architecture, integrating with Active Directory and adding a second factor at the logon layer.

Authentication factors for plant floor operators must be selected for physical reality. Hardware TOTP tokens — key-fob devices that generate a six-digit time-based one-time password every thirty seconds — are the most operationally reliable factor for environments where smartphones are impractical or prohibited. They require no smartphone, no data connectivity, no app installation, no language literacy for daily use. A six-digit code is universal across every Indian plant workforce.

For shift-based SCADA operations: enforce MFA at the start of a named operator session; hold the session active for the duration of the shift. Every action during that session is logged to the named individual. When the shift ends, the session closes. The audit trail is complete. The operational friction is minimal.

Level 3 — Site operations networks

Standard AD-integrated MFA. Cisco Duo integrates with Windows Active Directory and adds MFA at workstation logon, VPN access, and RDP sessions. This layer runs on Windows infrastructure and supports the same deployment model as corporate IT. Adaptive policies enforce step-up authentication for access to historian servers, MES applications, and network management interfaces.

Vendor and remote access — the highest-priority deployment target

Every external party accessing OT systems — SCADA integrators, PLC vendors, DCS service teams, OEM remote support — must access through a controlled gateway with MFA enforced, session recording active, credentials time-limited to the engagement window, and formal access decommissioning at engagement end.

Cisco Duo Network Gateway enables zero trust remote access to OT applications without requiring a VPN, enforcing MFA at the access layer before any session reaches the OT network. All sessions are logged to a named user and available for audit review. This is the single deployment that closes the vendor access gap responsible for a disproportionate share of Indian manufacturing breaches. It should be Phase 1, not Phase 3.

3.4 The break-glass procedure

Every MFA deployment in a manufacturing environment must include a documented, tested, and operationally viable break-glass procedure. Break-glass scenarios include MFA factor failure during a production emergency, an operator whose token is unavailable at a critical moment, and a network outage affecting authentication infrastructure during an active incident.

Cisco Duo supports bypass codes: time-limited, single-use codes generated by an administrator, providing controlled emergency access that preserves auditability without creating a permanent backdoor. The physical break-glass account is held in a sealed envelope in the plant manager's safe. Its use is a logged event that triggers immediate post-incident review.

What a tabletop exercise looks like in practice: once per quarter, the IT head, plant manager, and a shift supervisor run a 30-minute simulation. A scenario is stated: "SCADA operator cannot authenticate, alarm condition active, plant manager unavailable." The team walks through who holds the bypass envelope, who authorises its use, how the code is generated and communicated, and how the incident is logged. IEC 62443-2-1 explicitly requires break-glass account definition, secure storage, and usage logging as an OT access control requirement.

Section 4: Designing the Hybrid Plant Identity Architecture

4.1 The three environments that must be addressed

A complete MFA architecture for an Indian manufacturing enterprise addresses three distinct environments.

The IT environment

Corporate laptops, office workstations, business applications, email, ERP, cloud services. Standard enterprise MFA. Active Directory integration, adaptive policies based on device health and location. This layer is the most straightforward and should be the first phase for the corporate user population.

The OT environment

SCADA, DCS, HMI, historian, engineering workstations, PLCs. Differentiated by zone as described in Section 3. Hardware tokens, authentication proxies, session-based authentication for shift workers, zero trust remote access for vendors.

The hybrid boundary

MES platforms, plant-level historians with enterprise reporting, IoT gateways, remote monitoring platforms. This layer carries the highest lateral movement risk: corporate IT credentials can traverse the hybrid boundary into OT-adjacent systems without a segmentation barrier if the boundary is not governed. An attacker who compromises an IT credential through phishing, credential stuffing, or infostealer malware — and finds that the same credential provides access to an MES platform connected to the production network — has completed a breach pathway that bypasses every OT-specific control. The hybrid boundary is where that pathway is closed.

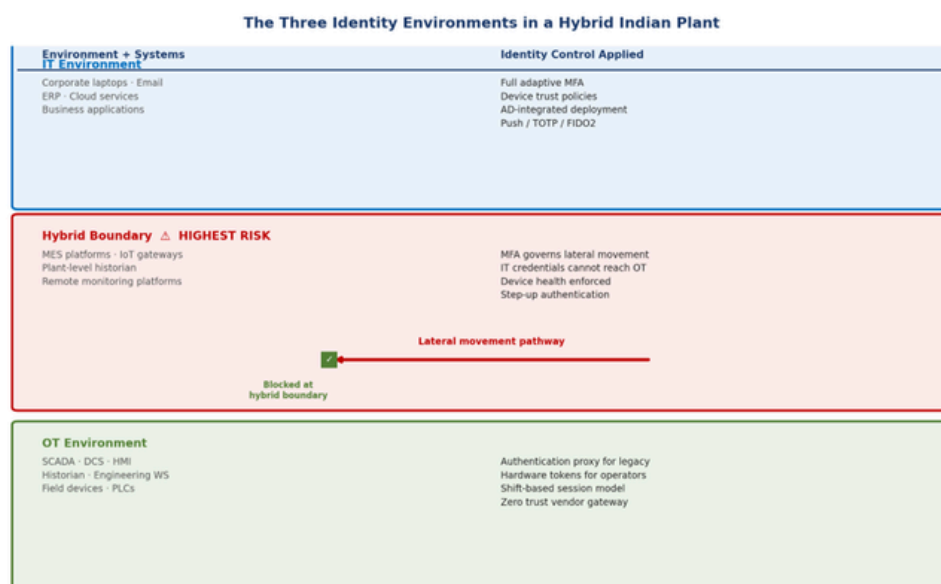


Figure 5: The Three Identity Environments in a Hybrid Indian Plant — and where lateral movement is blocked

4.2 Network segmentation as the companion control

MFA does not substitute for network segmentation. It complements it. Segmentation limits the blast radius of a compromised identity; MFA reduces the probability that any identity is compromised in the first place. Neither is sufficient alone.

For Indian manufacturers who have not yet segmented IT and OT networks, the sequencing is practical: deploy MFA for remote access and vendor sessions immediately. Build the segmentation architecture in parallel. The two projects do not need to wait for each other.

4.3 The device trust dimension

OT environments contain device categories that IT environments do not: engineering laptops that connect to both corporate Wi-Fi and the plant floor network, vendor-owned laptops brought on-site for maintenance work, ruggedised terminals on the shop floor that cannot support an MDM agent.

Cisco Duo's device health checks can enforce a minimum device security standard at authentication time: a device with an outdated operating system, missing encryption, or no screen lock can be blocked or stepped up before it reaches OT systems, regardless of whether the user credentials are valid. For vendor-owned devices — which cannot be managed through the manufacturer's MDM — a browser-based authentication flow requiring only the Duo Mobile application or a hardware token provides MFA enforcement without device enrolment. The session is scoped and time-limited.

Section 5: The Indian Manufacturing Context

5.1 The Pune-Chennai-Ahmedabad manufacturing corridor

The automotive and engineering clusters in Pune, Chennai, and Ahmedabad host large numbers of facilities with dense supply chain interdependencies. A credential compromise at a Tier-2 supplier can create access risk at the OEM through the simple fact that the same vendor holds active credentials in both environments. Global OEM customers are building cybersecurity requirements into supplier agreements. The MFA imperative for Indian manufacturers in these clusters is not just about protecting the plant. It is about preserving supplier status.

Pharmaceutical manufacturers in Hyderabad and Ahmedabad face an additional dimension: international market access. US FDA and EU EMA manufacturing site inspections are moving toward requiring documented cybersecurity controls for systems handling batch records and GMP-critical data. For defence and aerospace manufacturers in Bengaluru and Pune, DRDO and defence procurement guidelines are hardening on cybersecurity, with manufacturing partners handling sensitive technical data facing security obligations beyond standard commercial requirements.

5.2 The legacy system reality

No white paper on MFA for Indian manufacturing is honest if it does not acknowledge the legacy system reality. A significant proportion of Indian manufacturing infrastructure — particularly in process industries, chemicals, and older automotive plants — runs on OT systems that are 15 to 25 years old. These systems cannot be patched, cannot run modern

agents, and cannot natively support modern authentication protocols.

This does not make MFA impossible. It changes the implementation model. For legacy OT systems, MFA is applied at the network access layer rather than the application layer. An authentication gateway sits between the user and the legacy system, enforcing MFA at the gateway without requiring any modification to the legacy application. For a plant running 20-year-old SCADA infrastructure that cannot be replaced for five years, this is not a workaround. It is the correct architectural answer.

5.3 The workforce reality — the most India-specific section of this guide

Indian manufacturing plants employ a workforce with significant variation in digital literacy, device access, physical working conditions, and language. A corporate IT administrator in the Bengaluru office and a shift operator at a plant in Chhatrapati Sambhajnagar are both users in the identity system — but they are not the same user, and the authentication design must reflect that difference explicitly.

For plant floor operators who work in physically constrained environments — heavy gloves in press shops, restricted phone use in pharmaceutical or chemical environments, shared workstations in high-throughput production areas — hardware TOTP tokens are the correct factor. For supervisors and engineers, mobile push notification is efficient and well-suited to the role. For IT staff and managers across multiple sites, adaptive MFA with device trust enforcement and location-aware policies is the appropriate model.

The contractor and vendor enrolment challenge is the most commonly underestimated design problem in Indian manufacturing deployments. Consider the reality: a 200-person contractor workforce may include workers who have never used an authenticator app, who may not read enrolment instructions in English, and who are on-site for a three-week engagement before rotating out. The solution is a self-service enrolment flow with visual step-by-step instructions available in regional languages, a hardware token option as an alternative to smartphone enrolment, and a dedicated helpdesk contact for enrolment issues during the first 48 hours. A security control that is not adopted is not a control — it is documentation liability.

Workforce Segment	Physical Context	Recommended Factor	Session Model	Enrolment Approach
Plant floor operators	Heavy gloves, restricted phones, shift rotation, clean rooms	Hardware TOTP token	Shift-based; single logon per shift	Hardware token only; visual step-by-step instructions; local language support
Supervisors and engineers	Mobile across plant and office; device-diverse	Push notification (mobile); TOTP as backup	Standard session with idle timeout	Self-service app enrolment; IT helpdesk on call
IT staff and management	Multi-site; corporate devices; remote access common	Adaptive MFA; device health checks; push or TOTP	Standard + step-up for privileged access	Standard corporate enrolment flow
Contractors and vendors	Temporary; variable digital literacy; language diversity; BYOD	Hardware token or guided smartphone enrolment	Time-limited; scoped to engagement window; session recorded	Dedicated enrolment contact; visual guides; token as fallback; 30-day max credential window

Table 3: Matching MFA Factors to Indian Plant Workforce Segments

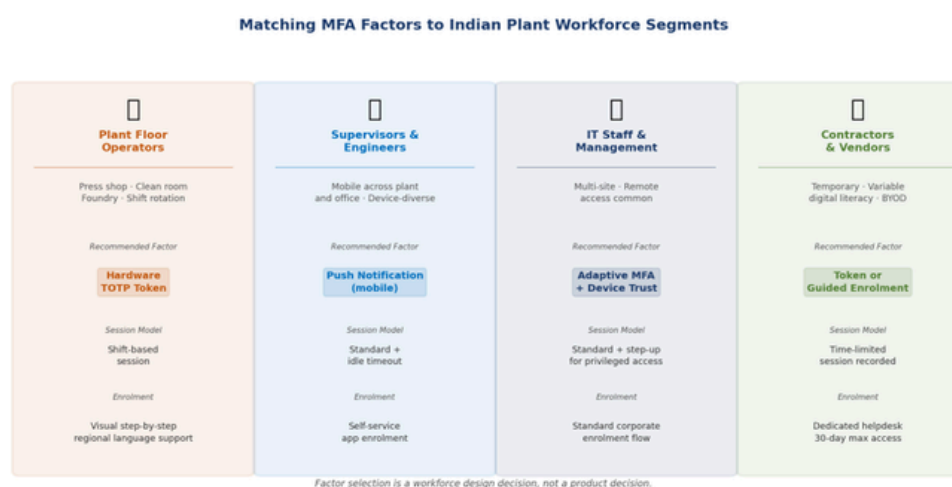


Figure 6: Matching MFA Factors to Indian Plant Workforce Segments

5.4 The OT security skills gap

Many Indian manufacturing enterprises — particularly mid-market players — do not have the internal security expertise to design, deploy, and operate an MFA architecture across a hybrid IT/OT environment. The OT security skills gap is real and acute nationally. Engineers who understand both SCADA architecture and identity security are scarce.

The practical responses are three: build internal capability over time through targeted training and certification (ISA/IEC 62443 certification programmes are available in India); engage a specialist implementation partner with documented OT security deployment experience; or adopt a managed identity services model. The relevant questions when evaluating a partner are not whether they can deploy Duo in an office environment. The questions are whether they have designed authentication proxy architectures for legacy SCADA systems, configured shift-based session models for HMI workstations, built vendor access gateways in OT DMZ configurations, and conducted break-glass tabletop exercises with plant operations teams.

Section 6: A Phased Deployment Roadmap

Phase	Timeline	Target	Key Actions	Outcome
Phase 1	Weeks 1–6	Remote access and vendor sessions	Audit and revoke shared VPN/OT credentials; deploy Duo for VPN; enforce MFA for all RDP; time-limit vendor credentials (30-day max); enable session recording; configure break-glass bypass; first tabletop exercise	Primary ransomware initial access vector closed; CERT-In audit readiness demonstrated
Phase 2	Weeks 4–12 (overlaps Phase 1)	Corporate IT and hybrid boundary	Deploy Duo with AD integration; enforce MFA at workstation logon; apply adaptive policies for MES/historian; enforce device health checks; map and govern hybrid IT/OT boundary	IT environment fully protected; lateral movement from IT to OT blocked at identity layer

Phase	Timeline	Target	Key Actions	Outcome
Phase 3 — Design	Weeks 8–12	SCADA and OT operational layer (design)	Map all SCADA/HMI authentication needs; design authentication proxy architecture; plan shift-session model; select and procure hardware tokens; define device trust policy for engineering laptops; validate break-glass for SCADA scenarios	Architecture validated before any OT change
Phase 3 — Deploy	Weeks 12–24	SCADA and OT operational layer (deployment)	Deploy authentication proxies for legacy SCADA; migrate shared accounts to named users; enrol plant floor operators on hardware tokens; configure shift-based sessions; deploy zero trust gateway for OT vendor access; test all paths under operational conditions	identity; full audit trail
Phase 4	Ongoing from Week 16	Continuous improvement and compliance	Quarterly access reviews; 30-day vendor account reviews; anomaly monitoring; break-glass tabletop exercises quarterly; IEC 62443 alignment; DPDP Act compliance documentation for May 2027 deadline	Sustained posture; audit-ready; supply chain qualified

Table 4: MFA Deployment Roadmap for an Indian Manufacturing Enterprise

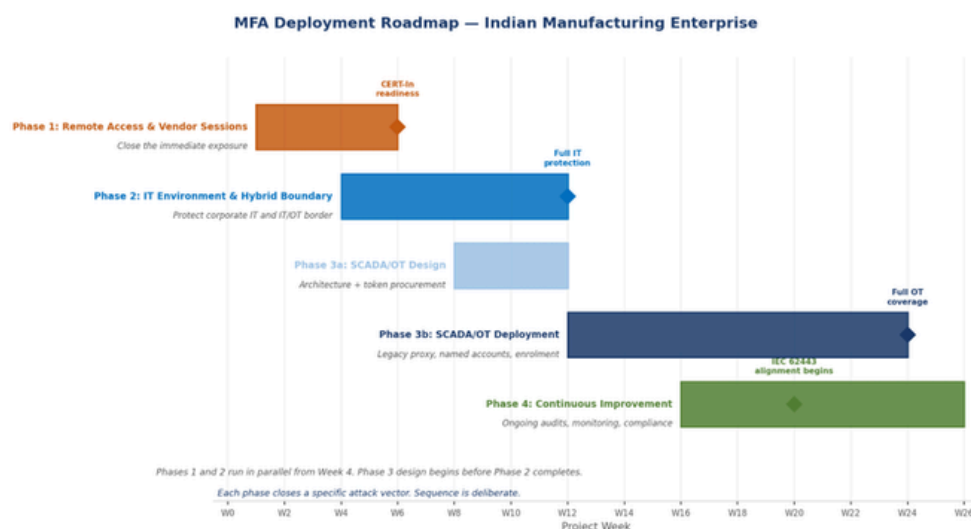


Figure 7: MFA Deployment Roadmap — Indian Manufacturing Enterprise (24-week phased rollout)

Phase 1 — Close the immediate exposure (Weeks 1–6)

Target: Remote access and vendor sessions. This is the highest-probability initial access vector, the most achievable deployment, and the one that delivers the most immediate risk reduction. It requires no changes to OT systems, no plant floor disruption, and no operator retraining.

Actions: Audit all active remote access credentials. Identify and immediately revoke all shared VPN accounts with OT access. Enumerate all vendor access accounts; confirm which are active and currently required. Deploy Cisco Duo for VPN authentication — every remote session into the plant network now requires MFA. Enforce MFA for all RDP sessions into OT-adjacent systems. Establish time-limited vendor credentials with a maximum 30-day active window. Enable session recording for all vendor remote access. Configure break-glass bypass codes and document the physical custody procedure. Run the first break-glass tabletop exercise before Phase 1 is considered complete.

Outcome: The primary initial access vector for manufacturing ransomware is closed. Every remote session is tied to a named identity. The organisation can demonstrate to CERT-In auditors that remote access is governed.

Phase 2 — Protect the IT environment and hybrid boundary (Weeks 4–12)

Target: Corporate IT, MES, historian, and IT/OT boundary systems. Deploy Cisco Duo with Active Directory integration across the corporate IT environment. Enforce MFA at workstation logon for all domain-joined machines. Apply adaptive policies for access to MES, historian, and cloud applications. Enforce device health checks for any machine accessing OT-adjacent systems. Map the hybrid boundary: identify every system that carries IT credentials into OT-adjacent access paths, and ensure MFA policy covers all of them.

Outcome: IT environment is MFA-protected. Lateral movement from IT to OT through the hybrid boundary is blocked at the identity layer.

Phase 3 — SCADA and the OT operational layer (Weeks 8–24)

Target: SCADA workstations, DCS consoles, engineering workstations, Level 2 and Level 3 OT systems. This is the most technically complex phase and requires the most design investment before deployment begins. Rushing it creates both security gaps and operational risk. The timeline is longer by design, not by delay.

Pre-deployment design work (Weeks 8–12): Map every SCADA and HMI system to its authentication model. Identify systems requiring an authentication proxy. Design the shift-session model for operator workstations. Select and procure hardware tokens for plant floor populations. Validate the break-glass procedure for SCADA-specific scenarios. Document the authentication architecture in a format presentable to an IEC 62443 assessor.

Deployment (Weeks 12–24): Deploy authentication proxies for legacy SCADA platforms. Migrate shared SCADA accounts to named user accounts — this is the operationally sensitive step and must be sequenced with shift operations. Enrol plant floor operators on hardware tokens. Configure shift-based session policies. Deploy zero trust remote access gateway for engineering and vendor access at OT levels 1 and 2. Test every authentication path under simulated operational conditions before going live.

The named account migration for SCADA operators is the highest-friction step in the entire deployment. Change management — explaining to operators why the shared login is being replaced and what to do if the token fails — is not a post-deployment task. It is a Phase 3 prerequisite.

Outcome: Every access to Level 2 and Level 3 OT systems is tied to a named, authenticated identity. The organisation has a complete, auditable record of who accessed what in the OT environment, when, and from which device.

Phase 4 — Continuous improvement and compliance alignment (Ongoing)

Quarterly access reviews and anomaly monitoring. Contractor and vendor account reviews at 30-day intervals. Break-glass tabletop exercises quarterly. Map MFA posture to IEC 62443 access control requirements as part of supplier qualification preparation. Align DPDP Act compliance documentation to identity security posture for the 13 May 2027 deadline.

Section 7: What Good Looks Like — The Target State

Every named individual — employee, contractor, vendor, or remote support engineer — who accesses any system in the IT or OT environment does so through a verified identity tied to a second factor. There are no shared accounts with production access. There are no standing vendor credentials that have not been reviewed in the last 30 days. There are no remote access paths into OT systems that bypass the authentication gateway.

Shift operators at Level 2 log on to SCADA workstations as named individuals using a hardware token. Their sessions are logged. Their access is scoped to the applications their role requires. When a shift ends, the session closes. When an operator leaves the organisation, the access is revoked and the removal is logged. The audit trail for any given access event is retrievable in minutes.

Vendors access OT systems through a controlled gateway. Their sessions are time-limited to the engagement window. Sessions are recorded and available for review. When the engagement ends, the account is disabled — not left dormant. The vendor cannot access the plant network at 2 AM three months after the project finished.

When a ransomware operator purchases a stolen credential on a dark web market, they obtain a username and a password. They do not obtain the second factor. The credential is worthless. The attack stops before it begins.

That is the value of MFA done properly in Indian manufacturing. Not a compliance checkbox. A production protection system.

Section 8: Key Statistics for Indian Manufacturing Security Leaders

For reference and internal communication use.

Statistic	Figure	Source
India manufacturing — weekly attacks per organisation	2,100+	Check Point Research, 2024
Manufacturing share of global industrial ransomware (Q1 2025)	68%	Dragos Year in Review, 2025
Indian manufacturers reporting multiple breaches in one year	55%	Industrial Cyber / survey, 2024
Average daily downtime cost — manufacturing ransomware	\$1.9 million (~₹15.8 crore)	Comparitech, 2024 (858 confirmed incidents)
Average time to restore operations after ransomware — manufacturing	30 days	Sophos State of Ransomware in Manufacturing, 2025
Average recovery cost (excl. ransom) — manufacturing	\$1.3 million	Sophos, 2025
Manufacturing organisations hit by ransomware globally (2024)	65%	Sophos, 2024
MFA blocks automated credential attacks	99%+	Microsoft research
Indian organisations at mature cybersecurity readiness	7%	Cisco Cybersecurity Readiness Index, 2025
Indian organisations unable to confirm if ever breached	73%	DSCI Cyber Threat Report, 2025
DPDP Act penalties (per contravention)	Up to ₹250 crore	Digital Personal Data Protection Act, 2023

Table 5: Key Statistics — Indian Manufacturing Cybersecurity and MFA

Conclusion: The Plant That Cannot Be Breached Through a Credential

Indian manufacturing is at an inflection point that every major industrial economy has passed through — the moment when digital convergence outpaces security governance, and a single credential compromise becomes capable of stopping production.

The solution to the most common initial access vector is known, deployable, and affordable relative to the cost of the incident it prevents. MFA, designed for the specific operational realities of OT environments — hardware tokens for plant floor operators, authentication proxies for legacy SCADA, shift-based sessions for continuous operations, zero trust gateways for vendors — closes the identity gap that attackers are actively exploiting.

The challenge is not technology. It is design. Building an authentication architecture that works for the SCADA operator in Pune, the remote vendor connecting from Bengaluru, and the IT administrator in the head office — while satisfying the IEC 62443 assessor and the CERT-In auditor — requires OT-specific expertise, not just IT security experience. That design challenge is solvable.

About Proactive Data Systems

Indian manufacturing is the second most attacked industry in the country, absorbing more than 2,100 cyberattacks per organisation per week. The attack vector has changed. It is no longer the perimeter. It is the identity layer — the shared accounts, the unmonitored vendor sessions, the remote engineering access that nobody formally decommissioned when the integrator finished the project eighteen months ago.

This white paper is written for the people who have to fix that: plant IT heads in Pune, security managers at automotive Tier-1s in Chennai, operations directors at pharmaceutical manufacturers in Hyderabad, and the CISO teams running hybrid environments where a 20-year-old SCADA system sits on the same network as a cloud-connected MES.

It covers why identity is the new perimeter in manufacturing, what MFA can and cannot do in an OT environment, how to design an authentication architecture that works across IT and OT without disrupting production, and what a phased deployment looks like for an Indian plant with realistic constraints.

Proactive Data Systems is an IT infrastructure and services company that designs, deploys, and supports secure, high-performance technology environments for organisations that cannot afford downtime. With over 35 years of experience, we have enabled more than 1,500 enterprises across India to modernise their networks, strengthen security, and scale with confidence.

Recognised as a Cisco Preferred Partner across Networking, Security, Collaboration, Cloud & AI, and Services. Proactive combines deep systems integration capability with disciplined delivery and managed services. Our expertise spans enterprise networking, cybersecurity, data centres, collaboration platforms, and structured cabling. We build and run infrastructure that performs reliably every day, not just at go-live.

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

 www.proactive.co.in

PROACTIVE™
Enhancing Digital Experience