



Digital Transformation for Energy Companies in India: ERP, EAM, Cybersecurity 2026

By Sudarshan Karweer · 25 August 2026 · growthifye.com

How Indian energy firms can use ERP, EAM, analytics, cloud and OT/IT cybersecurity to improve plant performance, compliance and returns in 2026.

India's power and renewable-energy sector is no longer debating whether to digitise. In 2026, the real question is where to place each rupee of digital spend so that it improves cash flow, asset availability, compliance, lender confidence and tariff competitiveness. For Indian C&I energy consumers, renewable developers, utilities, lenders and policymakers, the most practical digital stack is not a fashionable app layer. It is the operating backbone that connects ERP, EAM, analytics, cloud and OT/IT cybersecurity.

This matters because the economics of power projects are tighter than they look in headline announcements. Utility-scale solar tariffs discovered in recent bids have broadly stayed in the range of roughly Rs 2.45-3.20/kWh depending on location, offtake structure, storage integration and transmission assumptions. Wind and firm renewable products remain more case-specific, while C&I open-access supply often lands materially higher after banking, wheeling, cross-subsidy surcharge and balancing costs are included. In this environment, even a 0.5-1.5 percentage-point improvement in plant availability, a 1-2% reduction in auxiliary losses, or a 15-30 day reduction in receivables cycle can materially alter project IRR and debt-service resilience.

For energy companies, digital transformation should therefore be treated as an asset-performance and risk-management programme, not an IT procurement exercise. The most bankable digital initiatives are those that improve one or more of the following: generation yield, maintenance productivity, outage response, billing integrity, payment collection, regulatory reporting, cyber resilience and auditability.

Why the digital agenda has changed for Indian energy companies in 2026

Three structural shifts are driving a sharper focus on core systems.

First, asset fleets are getting more complex. Developers are managing combinations of centralised solar, wind, hybrid, BESS, RTC and FDRE-linked portfolios across multiple states. Each portfolio has different scheduling, dispatch, forecasting and settlement requirements. A developer with 1 GW spread across Rajasthan, ■■■■■■, Karnataka, Tamil Nadu and Maharashtra is not just operating plants. It is managing SLDC interfaces, curtailment patterns, OEM warranties, spares, evacuation constraints and increasingly granular performance guarantees.

Second, lenders and investors want cleaner operational data. Debt sizing and refinancing are increasingly influenced by the quality of generation history, downtime classification, receivables ageing, PPA compliance and maintenance records. Projects with weak data governance face slower diligence, more management adjustment questions and reduced confidence in reported performance ratios.

Third, cyber risk has moved from a technical issue to a board issue. As substations, inverters, SCADA, remote terminal units, billing systems and cloud analytics become interconnected, the attack surface expands. India's power sector already operates under stricter cyber directions, including compliance expectations shaped by the Central Electricity Authority's cybersecurity guidelines for the power sector, CERT-In directions and sector-specific critical infrastructure controls. In 2026, cyber preparedness is now linked directly to insurability, contractual risk and operational continuity.



ERP and EAM: the operating backbone, not back-office overhead

Many Indian energy firms still run plants with fragmented workflows: finance in one system, maintenance in spreadsheets, spare parts in emails, and performance analysis in disconnected dashboards. This creates hidden value leakage.

An integrated ERP and EAM architecture should answer a few practical questions every morning:

- Which assets are underperforming against irradiance or wind-resource conditions?
- Which work orders are overdue, and what revenue is at risk if they slip?
- Which critical spares are below threshold, and what is the lead time exposure?
- Which invoices are disputed, delayed or incorrectly billed?
- Which plants are non-compliant on safety, permit or cybersecurity actions?

For a renewable developer, the most useful ERP modules usually include finance and accounting, procurement, inventory, contract management, project controls and compliance tracking. EAM should cover asset registry, preventive maintenance, condition-based maintenance, mobile work orders, spare-parts planning, warranty tracking and failure-code analytics.

The business case is often underestimated. Consider a 250 MW solar portfolio with a blended CUF of 24%, annual generation of about 525 million kWh and realised tariff of Rs 2.80/kWh. Annual revenue is around Rs 147 crore. If better maintenance planning and parts availability improve net generation by just 0.8%, that is roughly 4.2 million extra kWh, or nearly Rs 1.18 crore of annual revenue before considering REC or other contract-specific factors. Add lower emergency maintenance, fewer truck rolls and tighter inventory control, and the digital payback can be very short.

For wind, the value can be even more pronounced because downtime events can be costlier and fault diagnosis more specialised. A 200 MW wind fleet at a 32% PLF generates about 560 million kWh annually. At Rs 3.20/kWh, every 1% gain in availability can equate to around Rs 1.79 crore in annual top-line benefit, subject to seasonality and curtailment conditions.

What should Indian firms prioritise in ERP/EAM implementation?

- Standard asset taxonomy across OEMs, sites and states
- Uniform downtime codes for true root-cause analysis
- Integration with SCADA, inverter, meter and weather systems
- Automated spare-parts reorder logic for critical equipment
- Digital approval workflows for procurement and capex variation
- Mobile apps for technicians working in low-connectivity locations
- Linkage between maintenance events and financial impact

A common mistake is implementing ERP as a finance-led compliance tool and EAM as a maintenance-only tool. In energy, they should be connected from day one because every maintenance action affects generation, billing and debt service.

Analytics that actually improve yield, not just dashboard aesthetics

Most power companies already have dashboards. Far fewer have decision-grade analytics.

The distinction is simple. A dashboard tells you that PR fell. A useful analytics system tells you whether the root cause was tracker stow logic, clipping, soiling, combiner-box trips, string mismatch, inverter derating,



high module temperature, grid curtailment or meter data quality.

In 2026, the strongest analytics use cases for Indian energy companies include:

- Yield-loss accounting at plant, block, feeder and inverter level
- Soiling and cleaning optimisation using local weather and generation loss curves
- Forecasting for scheduling and deviation settlement
- Curtailment detection and evidence logs for commercial claims
- Battery dispatch optimisation for hybrid and storage assets
- Receivables and collection analytics by DISCOM, offtaker and invoice class
- Portfolio-level benchmarking by OEM, site and contractor

For C&I open-access suppliers, forecasting and settlement analytics deserve special attention. As open-access and group-captive portfolios scale, deviation costs, banking limitations and demand-shaping become material commercial variables. A 50 MW hybrid portfolio serving industrial consumers can lose margin quickly if day-ahead forecasts are weak or if plant-level data is delayed. Better forecasting models, combined with machine-readable SLDC submissions and auditable logs, can reduce avoidable penalties and improve customer confidence.

For utilities and distribution companies, analytics priorities are somewhat different. The biggest gains usually come from feeder-level energy accounting, AT&C loss segmentation, transformer failure analysis, demand forecasting and outage restoration analytics. State utilities under RDSS-linked modernisation efforts have already invested in metering and IT layers; the next step is making those systems interoperable and usable for planning, not just reporting.

A practical KPI framework is better than a long list of vanity metrics. We recommend tracking a concise digital value scorecard:

- Plant availability
- Performance ratio or equivalent resource-normalised metric
- Mean time to repair
- Preventive maintenance compliance
- Critical spares stock-out incidents
- Forecast accuracy
- Billing cycle time
- Receivables days outstanding
- Cyber patch compliance
- Unplanned outage hours attributable to digital or communication failures

Cloud and digital platforms: where to centralise, where to stay local

Cloud adoption in the energy sector should be selective, architecture-led and security-aware. Not every workload belongs in the cloud, and not every site should keep data fully local.

The right model for most Indian energy companies is hybrid. Time-sensitive plant control functions should remain close to the asset edge. Enterprise systems, analytics, document management, collaboration and many integration services can sit in secure cloud environments, provided data flows are clearly designed and



compliance requirements are met.

Why does this matter commercially? Because platform fragmentation is expensive. A developer with separate systems for project execution, O&M, finance, land records, PPA documents, insurance, ESG reporting and site security ends up spending more on reconciliation than on insight. A digital platform approach can create a common data layer across the asset lifecycle:

- Development: land, permits, transmission status, contractor packages
- Construction: schedules, QA/QC, punch lists, change orders
- Operations: SCADA, work orders, inventory, warranties, incidents
- Commercial: invoicing, collections, PPA obligations, claims
- Financing: covenants, DSRA status, reporting packs, audits

For lenders, this is valuable because standardised digital reporting lowers diligence friction. For policymakers, it supports better system visibility. For developers, it improves internal control.

However, cloud strategy in power should address four practical issues from the start:

- Data residency and regulatory obligations
- Low-bandwidth or intermittent site connectivity
- Interoperability with legacy OEM systems and utility interfaces
- Disaster recovery and business continuity for mission-critical operations

A mature platform design also anticipates India's multilingual, multi-state operating reality. Site teams, DISCOM interfaces, contractors and local authorities often work across varying digital maturity levels. Systems must be usable in the field, not just by headquarters teams.

OT/IT cybersecurity: now a generation-risk and lender-risk issue

Energy cyber risk is no longer limited to the corporate email environment. In a renewable or utility setting, the highest-consequence incidents often involve the operational technology layer: SCADA servers, gateway devices, remote access tools, protection systems, substation automation and OEM maintenance connections.

The core problem in many Indian organisations is historical. OT systems were designed for availability and engineering functionality, not modern network exposure. As operators added remote monitoring, cloud analytics and third-party service access, connectivity increased faster than governance.

In 2026, a practical OT/IT cybersecurity programme for energy companies should include:

- Asset inventory for both IT and OT environments
- Network segmentation between corporate IT, plant networks and vendor access paths
- Multi-factor authentication for privileged and remote access
- Strict vendor access control with session logging
- Vulnerability management aligned with outage windows and OEM constraints
- Security monitoring for anomalous plant-network behaviour
- Backup and recovery testing for critical operational systems
- Incident-response playbooks that include plant operations, not just IT teams
- Tabletop exercises involving engineering, legal, communications and management



Boards often ask about ROI. Cyber ROI is difficult to model as direct revenue gain, but it is visible in avoided loss. A ransomware event or unauthorised remote access incident can trigger generation loss, dispatch disruption, forensic costs, contractual disputes and reputational damage. For utility-connected assets, the consequences can extend into regulatory scrutiny. For financed projects, lenders increasingly examine cyber governance alongside insurance, O&M capability and contract structure.

A sensible starting point is a cyber maturity assessment mapped to plant criticality. Not every site needs identical controls on day one. A 5 MW rooftop portfolio and a multi-state 2 GW hybrid fleet have very different exposure. But both need visibility, access discipline and tested recovery procedures.

Building the business case: what digital investment should be approved first

Indian promoters and CFOs are right to ask for prioritisation. Digital transformation can become expensive if it turns into software accumulation without process discipline.

We generally advise sequencing investments into three waves.

Wave 1: control and visibility

- ERP finance and procurement stabilisation
- Core EAM with asset registry and work orders
- SCADA and meter data integration
- Basic cybersecurity hygiene and access control
- Management dashboards tied to operational KPIs

Wave 2: optimisation

- Predictive maintenance models
- Forecasting and scheduling analytics
- Mobile field-service workflows
- Inventory optimisation
- Digital document control for contracts and compliance

Wave 3: advanced platform value

- Portfolio command centre
- Automated lender and investor reporting
- Battery optimisation for hybrid and storage assets
- AI-assisted anomaly detection with human review
- Enterprise-wide digital twin use cases where justified

The rule is simple: implement systems that improve core process integrity before funding sophisticated analytics. A poor asset hierarchy plus messy downtime codes will not produce good predictive insights, no matter how advanced the model.

For project-finance stakeholders, the strongest digital cases are those that support measurable risk reduction:

- Lower outage frequency
- Faster fault resolution



- Better spare-parts planning
- Cleaner billing and payment trails
- Stronger audit readiness
- Better cyber preparedness

These outcomes matter in refinancing, acquisitions, portfolio sales and dispute resolution.

What Indian energy firms should do in the next 12 months

In 2026, the most effective companies are not the ones with the largest software budgets. They are the ones with disciplined digital governance.

A realistic 12-month plan should include:

- Baseline current systems, data quality and cybersecurity posture
- Define a target operating model for development, O&M, finance and compliance
- Standardise asset naming, failure codes and reporting hierarchies
- Select ERP/EAM architecture based on integration needs, not vendor marketing
- Create a site-connectivity and edge-data strategy for remote plants
- Establish a cyber governance committee that includes operations leadership
- Launch 2-3 value-focused analytics use cases with clear financial metrics
- Build lender-ready and board-ready reporting packs from the same data backbone

For policymakers and utilities, the same logic applies at sector scale. Digital reform works best when standards, interoperability and cybersecurity expectations are clear. Programmes linked to grid modernisation, storage integration, advanced metering, renewable balancing and market design should be supported by robust data architecture, not isolated portals.

India's energy transition will not be delivered by generation capacity alone. It will be delivered by operationally disciplined, cyber-resilient and financially transparent companies that can manage increasingly complex assets at low cost. ERP, EAM, analytics, cloud and OT/IT cybersecurity are therefore not support functions. They are core infrastructure for bankable energy growth.

If your organisation is planning an ERP/EAM rollout, digital platform roadmap, analytics programme or OT/IT cybersecurity upgrade for energy assets in India, contact Growthifye's advisory desk for a practical assessment and implementation strategy.

ABOUT THE AUTHOR

Sudarshan Karweer — Chief Executive Officer, Growthifye

Over 23 years in management consulting — concept to scale — building and scaling new-age digital and energy businesses. An EY alumnus, Sudarshan leads Growthifye's renewable energy & storage advisory, EPC, transmission engineering and green-financing practices for developers, utilities and C&I consumers across India.
Contact: info@growthifye.com · +91 84510 99371 · growthifye.com

This article is for general information only and does not constitute engineering, financial or legal advice. © Growthifye. Sharing with attribution is welcome.