SCADA, DERMS and Renewable Control Centres in India 2026: IT Stack and ROI

By Sudarshan Karweer · 27 August 2026 · growthifye.com

How SCADA, DERMS and renewable control centres improve curtailment, scheduling, cybersecurity and ROI for India's energy sector in 2026.

India's renewable pipeline is growing faster than many operating models can handle. Solar parks, wind clusters, hybrid projects, C&I open-access assets, storage-linked plants and behind-the-meter portfolios are all adding telemetry, controls and scheduling complexity. Yet many owners still run operations on a patchwork of plant SCADA, inverter portals, OEM dashboards, spreadsheets and manual calls with SLDCs.

That setup may work for a single plant. It starts to fail when a developer manages 300 MW across multiple states, when a C&I portfolio must match generation against volatile load and open-access schedules, or when a lender needs confidence that generation losses, curtailment and grid events are being measured correctly. In 2026, this is exactly where renewable control centres, fleet-level SCADA and DERMS are becoming a practical IT priority in India.

This article looks at the Indian business case for central renewable control centres, the technology stack behind SCADA and DERMS, where the ROI actually comes from, and how developers, utilities, lenders and policymakers should assess these investments.

Why this topic matters in India in 2026

India's energy transition is no longer just about adding megawatts. It is about operating distributed and utility-scale assets with tighter commercial discipline. Several market conditions are driving this shift.

First, scheduling, forecasting and deviation settlement have become more material for both utility-scale and open-access portfolios. As renewable penetration rises, state and regional load despatch centres are increasing expectations around telemetry quality, visibility and response time.

Second, curtailment and grid unavailability remain real value leakages in several corridors. Even when a project cannot prevent all curtailment, a central control architecture helps classify losses correctly: plant outage, evacuation constraint, backing down instruction, communication failure, forecasting error or local equipment issue. That matters for claims, lender reporting and internal performance improvement.

Third, hybrid and storage-linked projects are changing the operating model. A solar or wind plant with a battery is no longer just a generation asset. It is a dispatch asset. The control layer must decide when to charge, discharge, respond to schedule revisions and maintain technical limits.

Fourth, C&I portfolios are getting more distributed. An industrial group may now have rooftop solar, captive solar, group captive wind, diesel backup, gas gensets, thermal loads and battery systems across sites. The operating question is no longer just generation monitoring. It is multi-asset coordination.

Finally, cybersecurity expectations have increased. As more renewable assets connect operational systems to enterprise networks and cloud analytics environments, the attack surface expands. Remote access to inverters, RTUs, weather stations and substation systems must be governed properly.

What a renewable control centre actually includes

In India, the term "control centre" is used loosely. In practice, there are three distinct but overlapping layers.

- Plant SCADA: site-level supervision, alarms, historian, local controls and OEM integration
- Fleet monitoring platform: centralized visibility across multiple plants, often cloud-enabled, with KPIs and reporting
- DERMS or portfolio control platform: optimization and coordinated control across distributed assets, storage, flexible loads and market-facing schedules

A serious renewable control centre combines these layers into an operational capability, not just a video wall.

The typical 2026 stack includes:

- Field layer: meters, protection relays, weather stations, PMUs where relevant, inverter and turbine controllers, BMS, PPC, RTUs and gateways
- Communications layer: fibre, MPLS, RF or 4G/5G links, edge buffering, secure protocols and network segmentation
- Control layer: SCADA servers, historians, alarm engines, event processing and command execution systems
- Integration layer: APIs, message brokers, OPC UA or IEC-based connectors, EMS links, scheduling systems and enterprise integration
- Application layer: forecasting, deviation monitoring, curtailment analytics, asset performance, energy accounting and maintenance workflows
- Security layer: identity controls, jump servers, logging, endpoint hardening, vulnerability management and SOC visibility

For larger portfolios, the control centre also connects to enterprise systems for ticketing, contracts, settlement, invoicing support and management dashboards. That is where Growthifye capabilities such as [Data & analytics platforms](/coreservices/itconsulting/dataandanalyticsplatforms) and Cybersecurity become directly relevant.

SCADA vs DERMS: what Indian buyers often misunderstand

A common error is to treat DERMS as just “advanced SCADA.” It is not.

SCADA tells you what is happening and allows supervisory control within defined boundaries. DERMS adds orchestration logic across many distributed assets. It can prioritize actions based on commercial and technical objectives, such as:

- meeting a day-ahead or intraday schedule
- minimizing deviation charges
- dispatching battery energy during expensive time blocks
- reducing export during network constraints
- coordinating curtailable industrial loads with onsite generation
- supporting feeder-level balancing or utility flexibility programs

For a 50 MW standalone solar plant, DERMS may be unnecessary. For a portfolio of 20 to 200 distributed assets with mixed ownership structures, variable offtake and storage integration, DERMS can materially improve both compliance and economics.

Utilities should view DERMS in the context of feeder visibility and distributed resource coordination. Developers should view it as a portfolio margin tool. Lenders should view it as a control and transparency

layer that reduces reporting ambiguity and operational slippage.

Where the ROI comes from in Indian projects

The strongest business case for central control platforms in India is usually not labour savings. It is avoided value leakage.

1) Lower generation loss from faster fault response

In many multi-site portfolios, mean time to detect and mean time to respond are still too high. If a 100 MW solar portfolio with a 24% CUF loses just 0.75% annual generation due to slow alarm handling and communication blind spots, that is about 1.58 million kWh per year.

At a realized tariff of Rs 3.20 to Rs 4.20 per kWh, that equals roughly Rs 50 lakh to Rs 66 lakh annually. A central alarm and dispatch process can recover part of this through better triage, escalation and OEM coordination.

2) Better curtailment classification and claims support

Suppose a 250 MW interstate renewable portfolio sees 2% to 4% annual energy impact from evacuation constraints, backing down events or schedule-related instructions in a stressed corridor. Even if only a fraction is commercially recoverable or useful in contractual discussions, credible timestamped event records are valuable.

Control-centre historians, synchronized event logs and automated curtailment tagging provide the evidence base. Without them, commercial teams often argue from incomplete data.

3) Reduced deviation and schedule mismatch costs

For open-access and hybrid portfolios, schedule error costs can be material, especially when weather changes rapidly or industrial demand shifts. A DERMS-linked control centre that integrates forecasting, schedule revisions and battery dispatch can reduce deviation exposure.

On portfolios where monthly deviation-related losses run into 0.5% to 1.5% of revenue, even a 30% to 40% reduction can justify the software and communications cost over a reasonable period.

4) Improved battery arbitrage and hybrid dispatch

In storage-linked systems, poor dispatch logic destroys value quickly. A battery cycled at the wrong hour, held in reserve unnecessarily, or dispatched without accounting for state of charge constraints can lose multiple paise per kWh at portfolio scale.

A robust control layer improves decisions around:

- charge from solar spill vs grid import
- discharge into evening peaks
- reserve margins for schedule compliance
- response to revised weather forecasts
- coordination with contractual offtake windows

On C&I sites where peak power costs, demand charges and backup fuel substitution matter, the economics can be even sharper than on utility-scale plants.

5) O&M productivity and spares planning

Fleet-level visibility helps standardize alarms, failure codes and work orders across OEMs. That supports better root-cause analysis and spare-parts planning. The value is not just fewer site visits, but better prioritization of critical visits.

For example, one truck roll avoided per plant per month across 25 sites can save meaningful cost. But more importantly, site teams can focus on high-loss issues rather than noisy alarms.

A practical Indian architecture for 2026 deployments

A workable design for India must account for communications variability, mixed OEM estates and uneven site maturity. Over-designed architectures often fail because field conditions are messy.

A pragmatic blueprint usually includes the following.

Edge-first resilience

Do not assume continuous high-quality connectivity. The edge layer should buffer data locally, maintain time synchronization and continue critical local controls if the central link fails.

OEM-agnostic integration

Many Indian portfolios include inverters, turbines and BESS systems from multiple vendors. The control centre must ingest data from Modbus, OPC, IEC 60870-5-104, IEC 61850 gateways and API-based OEM platforms where direct access is limited.

Hierarchical control authority

Command logic must clearly define what remains local at plant level, what can be executed centrally and what requires operator authorization. This is essential for safe operation and auditability.

Unified time-series historian

A single operational historian across plants materially improves event analysis, PR calculations, fault correlation and lender reporting. Timestamp quality matters. So does metadata discipline.

Cloud plus secure OT boundary

Analytics and reporting can sit in a cloud environment, but direct control paths should be carefully segmented. In many cases, a hybrid design is best: OT systems remain protected on segregated networks while enterprise analytics, dashboards and workflow tools leverage cloud elasticity. This is where [Cloud migration](/coreservices/itconsulting/cloudmigration) should be planned with OT realities in mind, not treated as a generic IT exercise.

Cybersecurity and compliance priorities

India’s energy asset owners can no longer treat renewable sites as low-risk digital environments. The combination of remote access, internet-exposed devices, contractor laptops and fragmented credentials is a serious weakness.

Minimum 2026 controls should include:

- network segmentation between enterprise IT and plant OT
- MFA for remote access and privileged accounts
- jump-host based administration instead of direct device exposure
- asset inventory across PLCs, RTUs, gateways, HMIs and networking gear

- patch and vulnerability governance aligned to operational windows
- central log collection for access and command events
- backup and recovery tests for SCADA and historian systems
- vendor access policies with session controls and approval workflows

From a board and lender perspective, this is not just an IT hygiene issue. It is directly tied to generation continuity, safety and insurability.

How different stakeholders should evaluate the business case

Developers should ask whether central control reduces avoidable losses across the portfolio and supports future complexity such as hybrids, storage and merchant exposure.

C&I consumers should evaluate whether integrated visibility across onsite and offsite assets reduces power procurement costs, demand peaks and schedule mismatch.

Utilities should focus on feeder visibility, distributed resource coordination, telemetry quality and response capability.

Lenders should assess data integrity, event traceability, cybersecurity maturity and whether operational reporting is sufficiently independent of fragmented OEM portals.

Policymakers should see renewable control centres and DERMS as enabling infrastructure for higher renewable penetration. As India moves toward more flexible systems, digital operational capability becomes as important as physical capacity addition.

Implementation pitfalls to avoid

Several control-centre programs in India underperform because they are approached as dashboard projects.

The common mistakes are:

- buying visualization without fixing field data quality
- ignoring communications redundancy in weak-connectivity locations
- relying excessively on OEM portals instead of building owner-controlled data access
- failing to standardize tags, alarms and event codes across plants
- not defining operating procedures for dispatch, escalation and curtailment logging
- treating cybersecurity as a later phase
- underestimating change management for plant operators and central teams

The better approach is phased execution with clear value targets. Start by securing telemetry, standardizing asset data and creating a reliable fleet historian. Then add alarm workflows, curtailment analytics and schedule monitoring. After that, introduce DERMS functions where the commercial case exists, especially for hybrid, storage and multi-site C&I portfolios.

This is also why [IT strategy & roadmaps](/coreservices/itconsulting/itstrategyandroadmaps) matter. Technology selection without an operating model, governance structure and value-capture plan usually leads to shelfware.

The 2026 outlook for India

By 2026, the question is no longer whether Indian renewable portfolios need better digital operations. The question is what level of control sophistication each asset class requires.

Standalone projects may still operate adequately with strong plant SCADA and centralized monitoring. But portfolios with geographic spread, mixed technologies, open-access complexity, storage integration or tighter lender scrutiny increasingly need renewable control centres with fleet analytics and selective DERMS functionality.

The economics are strongest where even small improvements in generation recovery, deviation reduction, battery dispatch or curtailment evidence translate into large annual rupee value. In a market where tariffs are often tight and financing discipline is unforgiving, these gains are strategically important.

India has built significant renewable capacity. The next layer of competitiveness will come from operating that capacity with better data, faster decisions and more secure control environments.

If you are evaluating a renewable control centre, fleet SCADA upgrade or DERMS roadmap for Indian assets, contact Growthifye’s advisory desk for a practical assessment of architecture, ROI, cybersecurity and implementation priorities.

Explore Growthifye's related capabilities

This analysis connects directly to our advisory practice: [IT strategy & roadmaps](/coreservices/itconsulting/itstrategyandroadmaps) · [ERP & asset management systems](/coreservices/itconsulting/erpandassetmanagementsystems) · [Data & analytics platforms](/coreservices/itconsulting/dataandanalyticsplatforms) · [Cloud migration](/coreservices/itconsulting/cloudmigration).

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