LumeTrax
Technical note

TECHNICAL NOTE · TRUST CENTER

OT / IT separated by architecture. Not by promise.

Mission-critical control never moves out of the deterministic SCADA boundary. Analytics, workflow, optimization, and assurance run *above* that boundary, in shared platform services. The separation is a first-order architectural constraint — not a sales-deck slide.

DETERMINISTIC

The OT layer is where the asset is protected. Always.

ARCHITECTURAL

The boundary is enforced in the design — not by configuration.

AUDITABLE

Network segmentation, RBAC, audit log — all evidenceable

OT / IT separation by architecture

The deterministic-control boundary is a first-order architectural constraint, not a product configuration.

Adding a feature on the platform side never compromises the deterministic side.
New OEM ecosystems are added inside ingestion — never inside control.
Network segmentation enforces the architectural boundary at the network layer in addition.

§ 1 WHAT STAYS IN OT

Mission-critical control is the responsibility of the OT layer.

Renewable assets sit on infrastructure that has to fail safely. Supervisory control, interlocks, and safety-critical command sequencing are owned by SCADA, PLC, RTU, and the on-site controller. Determinism is provable there. The failure mode is engineered, not negotiated.

Function	Why it stays here
Supervisory control · setpoints · curtailment	Latency-bounded loop. Local fallback if WAN drops. No platform dependency for safe oper
Interlocks, breaker logic, protection functions	Engineered to standards (IEC 61850, IEEE 1547 where applicable). Evidence trail per proj
Safe-state and shutdown sequencing	Site engineering authority. Reviewed by the IE / lender's adviser at engagement.
Edge data collection (Modbus, IEC 61850, SunSpec, OPC UA, OEM APIs)	Acquisition and buffering at the edge gateway. Buffered locally; replays the gap on reconnect.
BESS PCS, inverter, switchgear control	Vendor-native control logic. LumeTrax never closes the loop on these assets.

§ 2 WHAT RUNS ABOVE

Analytics, workflow, optimization, assurance — useful, valuable, never the layer protecting the asset.

Above the boundary, the platform consolidates measurement and operational data into one tenant hierarchy and one set of finance-grade definitions. Outputs are source-classified: MEASURED, CALCULATED, ASSUMED, and JUDGED are kept distinct end-to-end so the lender, the IE, or the insurer can see what came from which signal class without re-deriving the chain.

Service	What it does — and the boundary it respects
Analytics · performance	Contracted-vs-actual energy, loss-waterfall attribution, alarm pattern analysis. Read-only over the historian. No s
Workflow · asset manager	Tickets, SLAs, OEM warranty evidence packs, spares. Operates against telemetry and the configuration model –
Hybrid EMS optimization	Advisory dispatch envelopes for hybrid sites. The OT controller closes the loop locally; the optimizer never bypas
Audit & Assurance	Lender-grade reporting and methodology-versioned outputs. Reads measured + calculated + assumed + judged
Identity · RBAC · audit log	Enterprise SSO and MFA. Roles scoped to plant, subsystem, function, and authority level. Every action recorded

§ 3 HOW THE BOUNDARY IS ENFORCED

Architecture first, network second, contract third — three reinforcing layers.

The separation isn't a single control. It's three layers, each independently auditable. If any one layer were the only line of defence, the design wouldn't be enough. All three stack together.

Layer	Mechanism	What you can audit
1. Architectural	Platform services have no API surface that closes the super[illegible]	[illegible]
2. Network	OT and IT zones are separated at the network layer. Cross-b[illegible]	[illegible]
3. Contractual	Data-neutrality policy is verbatim in the customer DPA / MSA. [illegible]	[illegible]

§ 4 DEPLOYMENT SHAPE DOES NOT CHANGE THE BOUNDARY

Cloud, private, on-prem, or air-gapped — same software, four shapes, identical OT separation.

Cloud (multi-tenant)	Platform services on a managed cloud region. OT separation unchanged. Edge gateway buffers locally; forward-
Private cloud (single-tenant)	Isolated cloud deployment per customer organisation. Same operations team, separate data + infrastructure. Sa
On-prem	Customer-controlled deployment in customer or partner datacentre. Same OT separation. No cross-perimeter de
Air-gapped	On-prem with no inbound or outbound platform connectivity. Ingestion + operations work entirely inside the custo

§ 5 STANDARDS ALIGNMENT

The architectural choices map cleanly to the standards procurement and lender's IE teams reference.

Standard	Where it applies in this note
IEC 62443-4-1 (Secure development lifecycle)	Internal SDLC alignment — implementation in progress (Phase 1, 0–9 months). Source-tree b
IEC 61850 (Substation + DER communication)	Reference protocol for the OT-side acquisition layer. Edge gateway speaks IEC 61850 alongs
IEC 61724-1 (PV plant performance monitoring)	Drives the source-classification discipline above the boundary — measured vs calculated vs a
IEC 61400-26-1 (Wind plant availability)	Drives the availability-decomposition framework — recoverable vs permanent loss attribution
NIST SP 800-82 (ICS / OT security)	Cross-reference for OT/IT zoning, network segmentation, allow-list discipline, and incident res
NERC CIP (regional, North American BES)	Alignment available on request as part of the engagement scope — applicability determined p

Companion documents. Customer Security Pack (full procurement-grade detail including encryption, RPO / RTO, sub-processor list, pre-completed CAIQ + SIG). Architecture Brief (system overview from edge to platform). Both available at lumetrax.com/resources.