WHITE PAPER 08

A Reference Architecture for Cloud, Hybrid, and On-Premises Energy Data Boundaries

How to connect enterprise and operational energy information while preserving security, control, resilience, and deployment choice

GRIDSTROM Intelligence · August 2026 · Published

Executive decision takeaway: Deployment location should not define trust. A durable energy platform separates data, identity, policy, integration, analytics, and control planes so each can be placed and governed according to risk and operating need.

Executive Summary

Energy intelligence crosses enterprise IT, operational technology, cloud services, partner systems, mobile users, field devices, and critical facilities. Some data can move freely; other data is sensitive, regulated, contract-limited, high-volume, latency-sensitive, or safety-relevant.

The right architecture is rarely cloud-only or on-premises-only. It assigns each workload and data flow to a boundary based on purpose, sensitivity, latency, availability, control consequence, and recovery requirement.

Six architectural planes

The identity plane authenticates users, services, devices, and partners. The policy plane decides what they may do. The integration plane maps and moves information. The data plane stores transactional, document, master, and time-series records. The intelligence plane models, detects, forecasts, and recommends. The control plane issues and verifies operational instructions.

Separating these planes allows an organization to run analytics in cloud infrastructure while keeping local control at a site, or to retain sensitive records on premises while sharing approved decision outputs.

Cloud, hybrid, and on-premises patterns

Cloud deployment can accelerate portfolio analytics, collaboration, scaling, updates, and partner access. On-premises deployment can meet local control, sovereignty, isolation, legacy, or reliability requirements. Hybrid deployment distributes functions: site gateways normalize data and enforce local policy; cloud services manage portfolio intelligence; enterprise systems retain authoritative records.

The pattern should be explicit. ‘Hybrid’ is not a vague promise; it is a documented set of components, trust boundaries, flows, dependencies, and failover behavior.

Zero trust and least privilege

NIST zero trust guidance removes implicit trust based solely on network location. Every access decision should consider identity, resource, device or workload posture, policy, and context. The same principle applies whether a component is on premises or in the cloud.

Human users, APIs, devices, gateways, and partner services require distinct identities. Authorization should be scoped to the minimum data and action, with stronger controls for commands than for reads.

IT/OT segmentation and safe control

Enterprise analytics should not create an uncontrolled path into operational networks. Gateways, brokers, DMZ patterns, allowlisted flows, protocol breaks, monitoring, and local safety systems reduce consequence. Default credentials, shared accounts, flat networks, and undocumented remote access are unacceptable.

Local operations must fail safely when external links are lost. Queued data can synchronize later; protective and critical control should continue according to site design.

Data movement and residency

Classify information by sensitivity, ownership, retention, latency, and permitted destination. Minimize movement: send an aggregate or event when raw high-frequency data is unnecessary. Encrypt in transit and at rest, manage keys, log access, and document third-party processing.

Bi-directional synchronization requires conflict policy, replay, idempotency, schema versioning, reconciliation, and deletion/offboarding behavior. A data boundary is incomplete without an exit path.

Reference implementation sequence

First inventory systems, devices, identities, data classes, and control consequences. Define trust zones and prohibited flows. Establish identity and policy. Deploy read-only integration and observability. Add governed synchronization. Test recovery and offline behavior. Introduce recommendation workflows. Enable limited control only after threat modeling, authorization, simulation, and rollback tests.

Architecture review should ask not only ‘Can it connect?’ but ‘What happens when it is compromised, disconnected, misconfigured, outdated, or removed?’

Questions for Leadership

- Which data and control functions must remain local, and why?
- Does every service and device have a distinct identity and least-privilege policy?
- Can the site operate safely during cloud or network loss?
- Can data be exported and access fully revoked during offboarding?

GRIDSTROM Position

GRIDSTROM’s platform architecture connects financial intelligence, enterprise data, asset operations, governed workflows, and lifecycle transactions around persistent records and explicit decision rights. The objective is not to replace every trusted source system. It is to preserve context across systems so an investment decision can remain connected to delivery, operation, optimization, service, and replacement.

Sources

1. **NIST SP 800-207, Zero Trust Architecture.** https://doi.org/10.6028/NIST.SP.800-207 Defines zero trust concepts across on-premises and cloud environments.
2. **NIST SP 1800-35, Implementing a Zero Trust Architecture.** https://pages.nist.gov/zero-trust-architecture/ Provides implementation examples across on-premises, multi-cloud, and hybrid environments.
3. **CISA, Energy Sector.** https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/energy-sector Provides current critical-infrastructure context for the energy sector.
4. **CISA, OT Asset Inventory Guidance.** https://www.cisa.gov/resources-tools/resources/foundations-ot-cybersecurity-asset-inventory-guidance-owners-and-operators Describes foundational asset inventory and taxonomy practices for OT owners and operators.

5. CISA, IT/ICS Segmentation Advisory. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-083a Recommends robust segmentation between IT and ICS networks.

Editorial note: External requirements, market rules, standards, security guidance, and technology capabilities change over time. Deployment decisions should use the current authoritative source and the organization's applicable legal, regulatory, technical, and contractual review.