

Monitoring-Only by Design

Why analytics that cannot command the field can go in front of every desk in the utility

PRODUCT	Grid Data Enhanced Analytics
AUDIENCE	CISOs, OT security teams, operations leaders

The best picture of the grid often reaches the fewest people

Most utilities already hold the data for a shared, live picture of their networks. The GIS has the connectivity model. SCADA reports telemetry and events. AMI reports reads and meter events from nearly every premise. Joined together, that data answers questions for the control room, the planners, the gas and water operators, and the executives who set budgets.

Yet the tools that join it often stay with a small group of specialists. Planners work from exports. Gas and water teams keep their own spreadsheets. Executives see a monthly slide. The reason is rarely missing features. It is usually a capability the tool has that most of its users will never need: the ability to send a command to the field.

Why a command path makes broad rollout hard

Once a system can open a breaker, change a setpoint, or move a regulator, every account on it matters. That changes how the utility has to treat the whole product.

Security review gets heavier. The OT security team has to ask who can reach the system, from which networks, and what a compromised account could do. Under NERC CIP and similar frameworks, systems that can affect grid operations carry real obligations for access control, logging, patching, and change management. The utility's compliance team decides how any system is classified, but a command path pushes that decision toward the strict end.

Every user becomes a switching risk. Even careful people make mistakes. A planner exploring a what-if should never be one wrong click away from a live operation. Utilities answer with training, confirmation dialogs, and role restrictions. Each of those helps. None of them removes the possibility.

A setting is not a guarantee. Many products offer a read-only role or a license option that hides control functions. That is useful, but a setting can be changed, misapplied during an upgrade, or bypassed by an account with more privilege than intended. A careful security reviewer has to treat a disabled capability as a capability that still exists.

The result is predictable. Access narrows to the people who already hold control-system rights, and the rest of the utility goes without.

Principles of a monitoring-only approach

No command path, by architecture. The analytics product contains no function that sends a command to a field device. The capability is absent, not switched off. There is no role to misconfigure and no setting to flip, because there is nothing behind it.

Data flows inward. The product reads SCADA telemetry and events over the standard protocols utilities already run, such as DNP3 and IEC 60870-5-104. It reads AMI data and the GIS model. It listens to the field. It does not speak back.

The utility keeps the decision to act. Analytics will find things that need work. The right output is a request that enters the utility's own work process, where the utility decides whether to dispatch, when, and who goes.

Systems of record stay the utility's. Findings are reported beside the utility's records rather than written over them. The GIS, the CIS, and the work management system remain the authority.

Access follows need. With no switching risk on the table, the question of who gets access becomes who benefits from the information. For most utilities, that is nearly everyone.

What it looks like in practice

Grid Data Enhanced Analytics (GDEA) joins the utility's GIS connectivity model, live SCADA telemetry and events, and AMI reads and events into one live map, with real power-flow and hydraulic solvers across electricity, gas, and water. It is monitoring-only by design: there is no command path to the field, and that is enforced by the product's architecture rather than by configuration.

That makes it practical to put the same picture in front of every desk:

- **Control-room operators** see live telemetry and events on the connectivity model, alarm overlays, and equipment detail.
- **Planning engineers** use feeder capacity, voltage analysis, power flow, and a scenario sandbox where they can propose a change and see exactly what moves, in a model that cannot touch the field.
- **Gas and water operators** track unaccounted-for gas, regulator performance, a graded leak register, and minimum night flow per district.
- **Executives** see the same joined, solved picture on their own dashboard.

When GDEA finds something that needs attention, it works through the utility's process rather than around it. It shows the work already open on each asset beside the findings that still need attention, and can raise a request for work. GDEA requests. The utility always dispatches.

ILLUSTRATIVE EXAMPLE (HYPOTHETICAL)

The following scenario is hypothetical. During a hot afternoon, a planning engineer notices a feeder running close to its limit. In the scenario sandbox she models moving part of its load to a neighboring feeder and sees that both would stay within limits. She cannot perform that transfer from GDEA, and she does not need to. She raises a request with the finding attached. The control room, working in its own switching tools under its own procedures, decides whether and when to act. On the same afternoon, a regional director checks the same feeder on a dashboard, and a water operator confirms the pump station on that feeder is running normally. None of them needed control-system rights to see it, and the security team did not have to grant any.

Questions to ask any vendor

Whether you are evaluating GDEA or any other analytics product, these questions separate a monitoring-only design from a monitoring-only setting:

- Does the product contain any function that can send a command, setpoint, or switching operation to a field device?
- If control functions exist but are disabled, how are they disabled, and who can turn them back on?
- Is monitoring-only enforced by the product's architecture, or by a role, license, or configuration option?
- Which protocols does it use with the SCADA estate, and in which direction does data flow?
- When the analytics find a problem, does the product dispatch work, or hand a request to your process?
- Does it ever write back to your GIS, CIS, or other systems of record?
- Can your security team review the design and confirm these answers for themselves?

Closing

Broad access to grid analytics is a security decision before it is a software decision. When the tool has no way to act on the field, that decision gets simpler, and the planners, gas and water operators, and executives can finally work from the same picture as the control room.

PeriNimble builds software for systems that can't afford failure. Learn more about Grid Data Enhanced Analytics at perinimble.com/grid-data-enhanced-analytics/, or talk with our team at perinimble.com/contact/.

ABOUT PERINIMBLE

PeriNimble builds mission-critical grid data software for energy and utility companies. Founded in 2022 and headquartered in Bloomington, Minnesota, we support more than 15 million meters and over 1 billion interval reads per day in production.

Built for systems that can't afford failure. · perinimble.com · perinimble.com/contact