SOPHIZO

INDUSTRY PLAYBOOK · ENERGY & UTILITIES

The grid is no longer a network. It is a negotiation.

Agentic AI for grid orchestration, asset maintenance, and ESG-grade reporting.

PUBLISHED 2026 · **SOPHIZO RESEARCH**

Fractional AI & RevOps Leadership
sophizo.net

Renewables made the grid bidirectional. Static control loops cannot keep up.

Solar floods the line at noon. EVs spike demand at six. A storm takes a substation offline at nine. Agentic AI sits across SCADA, AMI, weather, and market feeds and acts within physics-based guardrails. Done well, it does not just lower cost. It lowers the probability of cascading failure.

Why this matters now

An AI Officer in energy does not pick a model. They design the boundary between human and agent authority on critical infrastructure. The audit artifact is as important as the algorithm.

> *Your DER mix doubled in 18 months. Did your control loop change at all?*

AI on the grid is regulated as critical infrastructure. The threat model includes nation-state actors.

Beyond the six global regimes, energy & utilities carries the overlays below. Each one has its own enforcement model and its own evidence expectation.

NERC CIP NERC CIP-015 + AI Operating Procedures

NORTH AMERICA, NERC **CRITICAL**

Applies to. AI in Bulk Electric System operations, grid forecasting, demand response.

Key obligation. Critical infrastructure protection. CIP-015 internal network security monitoring. AI used in operating decisions inherits CIP-005 and CIP-007 obligations.

Evidence. CIP compliance documentation, AI model registry, incident response artifacts.

FERC AI FERC Order 2222 + RTO AI Market Surveillance

UNITED STATES, FERC **HIGH**

Applies to. AI in wholesale electricity markets, DER aggregation, congestion management.

Key obligation. Market manipulation rules apply to AI-driven bidding. Transparency for AI used in market participation.

Evidence. Bidding algorithm documentation, market surveillance logs, compliance attestations.

CSRD AI EU CSRD + ISSB + AI in ESG Reporting

EU + GLOBAL **ELEVATED**

Applies to. AI used in ESG data collection, emissions calculation, climate scenario modeling.

Key obligation. Auditable AI-generated ESG data. Disclosure of AI methodologies under CSRD ESRS.

Evidence. Methodology documentation, audit-ready ESG calculation traces, assurance reports.

NRC AI NRC AI Strategic Plan + Nuclear AI Guidance

UNITED STATES, NRC **CRITICAL**

Applies to. AI in nuclear plant operations, predictive maintenance, fuel management.

Key obligation. AI in safety-related systems requires formal qualification. 10 CFR 50 Appendix B quality assurance applies.

Evidence. Qualification documentation, V&V reports, regulatory engagement records.

Global emphasis for this sector. EU AI Act · NIST AI RMF · ISO/IEC 42001.

Four capability domains. One operating layer.

01 Smart-Grid Orchestration

- DER integration and dispatch agents
- Demand-response optimization
- Outage prediction and crew routing
- Physics-based guardrails on every action

02 Predictive Maintenance for Distributed Assets

- Vegetation-management agents using imagery
- Transformer health and replacement planning
- Substation-level anomaly detection
- Storm-hardening prioritization

> *If a substation went silent for 90 seconds tonight, what would the agent do, and would the operator know?*

Capability domains, continued.

03 Sustainability and ESG Reporting

- Continuous emissions accounting
- SASB, GRI, and CSRD-ready report drafting
- Scope-3 supplier-data agents
- Climate-disclosure assurance prep

04 Customer and Field Operations

- Outage-communications agents
- Field-tech dispatch optimization
- Bill-shock prediction with proactive outreach
- Multilingual customer agents

What production deployments look like at scale.

15 to 40%
OPERATIONS COST REDUCTION

150 to 250%
PRODUCTION ROI

12 to 18 mo
PAYBACK OFFSET BY ENERGY SAVINGS

Production-stage benchmarks compiled from Deloitte 2024 Power & Utilities Outlook, EIA Annual Energy Outlook and IEA World Energy Outlook reporting, and DOE Grid Modernization Initiative reporting. Your spread depends on AMI penetration, SCADA modernization stage, and DER mix.

The AI Officer Mandate.

Three responsibilities a Fractional AI Officer owns from day one in energy & utilities.

01
Physics-based guardrails so an erroneous agent action cannot destabilize a region.

02
ESG-grade audit trail aligned to CSRD, SASB, GRI, and SEC climate-disclosure rules.

03
Critical-infrastructure security. Agent identity, network segmentation, and adversary-aware monitoring.

06 · A 90-DAY PATH

How a Sophizo engagement starts in Energy & Utilities.

DAYS 1 TO 30

Diagnose

MAP THE OPERATING REALITY

- AI system inventory across the operation
- Risk and value-tier mapping by use case
- Vendor and integration audit
- Board-ready findings memo

DAYS 31 TO 60

Architect

DESIGN THE AUTONOMY BOUNDARY

- Agent permissions and escalation policy
- Evidence file and audit trail design
- First production pilot scoped with rollback plan
- Cross-functional governance committee charter

DAYS 61 TO 90

Operate

SHIP AND INSTRUMENT

- First agent in production with HITL controls
- Operator coaching and policy refinement
- P&L instrumentation by use case
- Quarterly review cadence established

What we will not do.

We do not own your NERC CIP compliance, run your DR program, or manage your trading desk. We do not recommend agent authority on any action that could trigger a frequency event, regardless of model accuracy in shadow mode. We pass on utilities where IT and OT operate as separate kingdoms with separate vendors, because grid-touching agents do not survive that boundary.

07 · WHAT THE BOARD NEEDS TO HEAR

Five things the board needs to hear about AI on the grid.

Five cited insights for the next risk-committee meeting. Each one is sourced. Each one is what an experienced AI Officer would put in front of the board if they walked in tomorrow.

01 · FEDERAL BASELINE

DOE's AI Risk Profile is the new floor for grid-touching AI.

DOE's October 2024 AI Risk Management Profile for the Energy Sector extends NIST AI RMF with sector-specific control families. FERC and NERC have signaled they will reference it in audits. Utilities running pilots without alignment now face a known gap, not an unknown one.

Source. DOE Office of Cybersecurity, Energy Security, and Emergency Response, AI Risk Management Profile for the Energy Sector, October 2024.

02 · NERC CIP SCOPE

Agentic AI touching the Bulk Electric System is already in CIP scope.

NERC CIP-002 through CIP-014 apply to any system that can affect Bulk Electric System reliability. Agents in dispatch, demand response, or SCADA orchestration are in scope by default. NERC's 2024 ERO compliance report indicates many utilities have not yet documented this.

Source. NERC CIP Standards (current); NERC 2024 ERO Enterprise Compliance Monitoring Report.

03 · DER PHYSICS

Distributed solar broke the static control loop.

EIA's 2024 Annual Energy Outlook reports US distributed solar capacity grew roughly 32 percent in two years. Most utilities still run quasi-static dispatch optimization designed for one-way flow. The optimization layer needs an agentic rewrite. The protection layer must not.

Source. EIA Annual Energy Outlook 2024; Lawrence Berkeley National Laboratory, Tracking the Sun: 2024 Edition.

Two more, then the framework.

04 · DISCLOSURE RULES

Climate disclosure is no longer just an SEC question.

The SEC's March 2024 climate disclosure rule is stayed pending litigation, but California SB 253 and the EU CSRD require the same underlying data. The reporting agents your CFO needs are still required by other regimes, regardless of how the SEC matter resolves.

Source. SEC Climate Disclosure Final Rule (March 2024, stayed); California SB 253 and SB 261 (2023); EU Corporate Sustainability Reporting Directive.

05 · WILDFIRE ECONOMICS

Wildfire liability turned vegetation-management AI into table stakes.

PG&E's Camp Fire liability cost 30 billion dollars. Insurance markets now price vegetation-management capability into utility cyber and operational coverage. Imagery-based inspection agents have shifted from discretionary to underwriting requirement in the highest-risk territories.

Source. California Department of Insurance 2024 Utility Loss Reports; Edison Electric Institute 2024 Wildfire Mitigation Survey.

The Grid Negotiation Layer.

A modern grid is a continuous negotiation between generation, load, weather, and price. Agents either join the negotiation under physics-based rules or they do not get to act. The guardrail layer is non-negotiable.

RULE 1

Thermal limits

Hard-coded per asset class and jurisdiction. Agent cannot cross.

RULE 2

Voltage and frequency

Envelopes pre-defined. No agent action that approaches the edge.

RULE 3

Contingency check

Pre-check before any state change. N-1 minimum, N-1-1 for critical assets.

RULE 4

Audit before commit

Artifact written before action executes, not after.

RULE 5

HITL on frequency events

Human authority on anything that could trigger a frequency event.

From John Utley.

> *Grid agents either operate inside physics or they do not operate. I do not care how accurate the model was in shadow mode. The first frequency event from an unsupervised agent will end the program, and it should. Build the guardrail layer first. The optimization comes second.*

John Utley

FOUNDER, SOPHIZO · SEATTLE, WA

John Utley founded Sophizo to give growth-stage companies the AI and revenue architecture work historically reserved for the Fortune 500. He writes and advises on agentic AI governance, predictive forecasting, and operating-model design for boards and operators across energy & utilities and adjacent sectors.

Test your operating picture against these.

1

Your DER mix doubled in 18 months. Did your control loop change at all?

2

If a substation went silent for 90 seconds tonight, what would the agent do, and would the operator know?

3

Outage durations dropped 9% YoY. Was that the weather, or the work?

Frequently asked questions.

How do you prevent agents from making destabilizing decisions?

Every grid-touching action passes through physics-based guardrails: thermal limits, voltage envelopes, frequency tolerances, contingency analysis. The agent cannot cross a guardrail. If it tries, it escalates and waits.

Will this satisfy regulators and ESG auditors?

Yes. We design the audit artifact alongside the agent. Every emission, every dispatch decision, every customer commitment generates a record an auditor can replay end to end.

How do you handle SCADA modernization?

We do not make SCADA modernization a prerequisite. We integrate read-only first, prove value, then make the case for the deeper integration with a P&L attached.

If this maps to your operating reality, we should talk.

The Diagnostic Sprint is two weeks. Board-ready output. Tailored to energy & utilities.

ENGAGE
sophizo.net/checkout/diagnostic-sprint

INDUSTRY PAGE
sophizo.net/industries/energy-utilities

EMAIL
john@sophi

12 · SOURCES

Primary research behind this brief.

Every claim, statistic, and citation in this playbook traces back to one of the primary sources below. Pressure-test any of them with your team. We have done the same.

01. US Department of Energy.

AI Risk Management Profile for the Energy Sector, October 2024.

02. North American Electric Reliability Corporation.

CIP Standards (current edition).

03. North American Electric Reliability Corporation.

2024 ERO Enterprise Compliance Monitoring and Enforcement Report.

04. US Energy Information Administration.

Annual Energy Outlook 2024.

05. Lawrence Berkeley National Laboratory.

Tracking the Sun: 2024 Edition.

06. US Securities and Exchange Commission.

Final Rule on Climate-Related Disclosures, March 2024.

07. California Department of Insurance.

2024 Utility Loss Reports.

08. Edison Electric Institute.

2024 Wildfire Mitigation Survey.

Editorial note. This brief is a field reference compiled by Sophizo Research. It is not legal, accounting, or clinical advice. Cite the primary regulator guidance for binding interpretation. Where statistics are quoted, the most recent published figure as of early 2026 is used.