



# SagaUtilityOps™

The Governed Operating Fabric  
for the Regulated Utility

*Executive Briefing · Confidential*

PraSaga Foundation | 2026



SagaUtilityOps™ | PraSaga Foundation | Confidential

20

Domain Modules

18

Sector Pain Points

43

Governed Classes

# A Utility Carries Institutional Obligations It Cannot Currently Prove



## Regulatory

Rate cases, FERC audits, and NERC CIP inspections require evidence assembled manually from disconnected systems — at enormous cost in counsel time and management attention.



## Litigation

Wildfire liability, interconnection disputes, and billing challenges turn on evidence quality. Post-incident reconstruction is expensive, slow, and defensively weak.



## Operational

Policy, tariff, contract, and authority constraints are enforced by institutional memory — not by the operating systems. Violations are discovered after execution, not prevented at it.



# SagaUtilityOps™: What It Is and What It Is Not

## ✓ IT IS

- ✓ **Governed evidence layer** — signed attestations and Merkle roots on chain; bulk OT data stays off-chain
- ✓ **Utility state machines** — policy, tariff, authority, and obligation gates before institutional transitions
- ✓ **Real-time supervisory fabric (SagaIoT)** — pub/sub, presence, engagement rules, MQTT + XMPP; supervisory commands at human/seconds scale
- ✓ **Governed actuation path (SagaAIoT)** — material commands policy-checked on SagaChain, then delivered over XMPP or MQTT
- ✓ **Sits above EMS, OMS, MDM, CIS** — integrates; Phase 1 does not replace OT/IT systems of record

## ✗ IT IS NOT

- ✗ **Sub-cycle protection or market clearing** — relays and ISO commitment stay in OT/market systems
- ✗ **Your CIS or billing engine** — governs determinants and evidence CIS consumes
- ✗ **A wholesale re-clearing engine** — reconciles ISO/RTO statements; doesn't run the market
- ✗ **Bulk meter data on a blockchain** — AMI intervals → data lake; anchor the window root when it matters legally

*Your OT stack runs the grid. SagaAIoT moves supervised data and commands at speed. SagaUtilityOps governs the evidence that obligations were met — defensible to the PUC, NERC, and the court.*



# Derived from 18 Documented Sector Pain Points

### Interconnection Queue

Multi-year backlogs → governed lifecycle

### Large-Load / Data Center

AI load shock → cost-allocation evidence

### DER / FERC 2222

DER proliferation → governed registration & M&V

### AMI / Metering VEE

Interval data → audit-ready determinants

### Outage & Restoration

OMS events → PUC-grade evidence

### Reliability Metrics

SAIDI/SAIFI → governed MED exclusion

### Wholesale Settlement

ISO statements → reconciled audit trail

### Demand Response M&V

Baseline disputes → governed methodology

### Tariff Governance

Schedule versions → approval-bound library

### Rate Case Proceedings

Docket chaos → governed proceeding state

### Asset Inspection

Field records → EAM-linked evidence

### Vegetation / Wildfire

Ignition risk → litigation-grade records

### Environmental / RPS/REC

Attribute certificates → provenance & retirement

### Emissions / PHMSA

Methane & pipeline integrity evidence

### NERC CIP Compliance

BES Cyber → structural enforcement, no gaps

### EV / Managed Charging

Load growth → governed enrollment & dispatch

### Customer Programs

Incentive programs → audit-ready disbursement

### CIM Network Model

Model changes → governed approval chain

### Power Procurement / PPA

Contract lifecycle → obligation & delivery evidence

### Attestation / SagaloT

OT data boundary → hash-anchored integrity



# Four Outcomes That Change the Risk and Cost Profile



## Regulatory Defense at Lower Cost

Evidence produced as operational output eliminates post-hoc reconstruction. The rate-case exhibit that took three weeks becomes a governed query. The CIP evidence packet that required six consultants is produced in hours.



## Litigation Risk Reduction

Wildfire liability, interconnection disputes, and billing challenges turn on contemporaneous, signed, timestamped evidence. SagaUtilityOps™ produces that evidence during normal operations — not under litigation pressure.



## Operational Integrity Across the Enterprise

Policy, tariff, contract, and authority constraints are enforced structurally. A transition cannot be recorded as complete until every approval, evidence element, and constraint is satisfied — prevention, not detection.



## Capital and Rate Case Positioning

Auditable operational governance improves rate-case posture, ESG reporting credibility, and credit market positioning. The platform cost is a recoverable regulatory asset with a quantifiable actuarial risk-reduction value.

# Operating Cost and Risk Before and After

| Cost Driver                      | Current State                                                | SagaUtilityOps™ State                                             |
|----------------------------------|--------------------------------------------------------------|-------------------------------------------------------------------|
| Rate case evidence prep          | 3–6 months, multiple consultants, external counsel           | Days to weeks — governed query against ledger                     |
| FERC / NERC audit response       | 6–10 weeks, significant outside counsel fees                 | Pre-built evidence packets — hours, not weeks                     |
| Wildfire litigation evidence     | 18+ months post-incident reconstruction, high exposure       | Contemporaneous, GPS-anchored, signed — produced during ops       |
| VEE billing dispute resolution   | Manual reconstruction per dispute, per meter, per period     | Audit-ready determinant trail — query-based retrieval             |
| DR M&V contested settlement      | Contested baseline methodology, external arbitration risk    | Governed methodology record, signed evidence, defensible          |
| NERC CIP evidence gaps           | Discovered during audit — enforcement risk, penalty exposure | Structural enforcement — gaps prevented at execution              |
| Interconnection queue management | Email, spreadsheet, multi-party coordination overhead        | Governed lifecycle — milestone tracking, cost-allocation evidence |



# Why Existing Approaches Leave the Gap Open

## Point Solutions

Separate trackers for interconnection, VEE, CIP. No cross-domain evidence thread. Rate case and litigation still require manual assembly.

**Incomplete**

## Enhanced ERP (SAP / Oracle)

ERP governs financial transactions. Does not produce governed state transitions or chain-of-custody evidence for operational decisions made outside the financial ledger.

**Wrong Layer**

## GIS + Document Management

Stores records. Does not enforce governed state transitions or produce chain-of-custody evidence automatically. Reconstruction cost unchanged.

**No Governance**

## Spreadsheets & Manual Binders

Not defensible at scale. Exposed to personnel turnover, version inconsistency, and post-incident reconstruction cost in litigation.

**Liability**



## SagaUtilityOps™

Governed state transitions across all 20 utility domains. Evidence produced as operational output. Inherits full enterprise and financial governance fabric. Sits above existing systems — no OT replacement required.



# Three Convergent Forces Demand Action



01

## The Regulatory Environment Has Changed Permanently

- Performance-based ratemaking is expanding in every jurisdiction
- FERC Order 2222 and DER market rules add compliance layers existing systems cannot track
- State climate mandates create new obligations faster than utilities can govern them
- Evidence rigor that was aspirational is now required and enforced



02

## The Litigation Environment Has Changed Permanently

- A single utility-caused ignition can exceed \$1B in wildfire liability
- Inverse condemnation in fire-risk states makes reconstruction-based evidence insufficient
- Interconnection and billing disputes increasingly turn on documentary evidence quality
- No utility in a fire-risk territory can afford to manage this evidence in spreadsheets



03

## The Technology Inflection Point Has Arrived

- SagaChain™ is a purpose-built institutional blockchain — not a general-purpose ledger retrofit
- SagaloT™ provides the OT/IT semantic fabric that bridges real-time operations and the governance layer
- The platform is already deployed in enterprise and financial verticals — utility extension, not greenfield
- The cost of inaction compounds; the cost of adoption is a recoverable regulatory asset



# Three Phases, Zero OT Disruption

## Phase 1

### Foundation & High-Priority Domains

- General governance core — inherited from EnterpriseOps and FinOps fabric
- Interconnection governance & large-load domain
- Metering / VEE integrity — billing determinant audit trail
- Outage evidence — OMS normalization to PUC-grade records
- NERC CIP or Vegetation/Wildfire — based on regulatory and geographic risk profile

*Highest-risk domains first. Immediate regulatory and litigation value.*

## Phase 2

### Market & Financial Integration

- Wholesale settlement reconciliation — ISO/RTO statement audit
- Rate case proceeding governance — docket lifecycle management
- Tariff lifecycle management — versioned, approval-bound schedule library
- Demand response M&V — baseline methodology and performance evidence
- DER / FERC Order 2222 compliance

*Connects to existing financial and regulatory reporting stack.*

## Phase 3

### Full Domain Activation & AI Governance

- EV / managed charging enrollment and dispatch evidence
- Environmental attribute (REC / carbon) provenance and retirement
- Customer program governance and incentive audit trail
- CIM network model governed change control
- SagaAI™ governance layer — deterministic pre-commit sufficiency checks

*Full platform activation. SagaAI™ provides AI-agent oversight for high-stakes decisions.*



# Governing AI That Acts on Your Infrastructure

## The Ungoverned AI Gap

DERMS dispatches DER assets automatically. Grid automation executes at machine speed. PSPS algorithms run before humans can review each action. These AI systems operate today without a verifiable authorization layer — no policy gate, no pre-execution record, no mechanism to block commands exceeding approved scope.

## Regulatory Alignment

- NERC CIP: pre-execution authorization records for automated BES control
- EU AI Act: policy gate + human oversight + pre-execution audit trail
- NIST AI RMF: provable governance controls, not self-attestation
- FERC 2222: dispatch authorization trace for DER aggregation



### The Policy Gate

Every AI command evaluated against policy before the device receives it. Commands that fail are blocked — not logged after the fact. Enforcement, not observation.



### The Permanent Record

Authorization and audit record created before the device acts. Single correlated record: policy, identity, time, device confirmation. Tamper-proof. Available on demand.



### Governed Playbooks

Multi-step sequences — DERMS dispatch, PSPS workflows, protection coordination — run step by step. Each step policy-checked, audited, human-gated where required.



### Human Oversight

Configurable per command type and per step. Routine commands proceed. Safety-critical setpoint changes pause for named human approver. Supervised, not unsupervised, automation.



# Post-Quantum Cryptography: Protected from the Start



## Harvest-Now, Decrypt-Later: The Active Threat

Adversaries capturing encrypted evidence records today can decrypt them when quantum capability arrives. Rate-case filings, PPA contracts, and asset inspection records that must remain cryptographically valid for 20–40 years are at risk from encryption deployed today.

### NIST Standards — In Force Now

|                           |                                                         |
|---------------------------|---------------------------------------------------------|
| <b>FIPS 203 (ML-KEM)</b>  | Quantum-safe key encapsulation — node-to-node transport |
| <b>FIPS 204 (ML-DSA)</b>  | Lattice signatures — primary validator vote signing     |
| <b>FIPS 205 (SLH-DSA)</b> | Hash-based signatures — conservative long-horizon layer |
| <b>FN-DSA / Falcon</b>    | Bandwidth-optimized lattice sigs for shard consensus    |

### SagaChain™ PQC Architecture

#### Quantum-resistant from block one

Not a planned upgrade — ML-DSA / FN-DSA consensus by architecture

#### ML-KEM transport layer

Node-to-node comms quantum-safe, not just ledger records

#### Hash-based meta-layer

SLH-DSA conservative fallback for decades-long evidence records

#### Crypto-agility built in

Algorithm rotation via XBOM governance policy — no hard fork required

The evidence records your utility creates today must remain cryptographically trustworthy for 30+ years. SagaChain™ is the only utility governance ledger designed for that lifecycle from day one.





PraSaga Foundation

# SagaUtilityOps™

*The institutional imperative:*

The regulated utility must be able to prove, with chain-of-custody precision, that every obligation it carries was honored — in real time, not in retrospect.

**SagaUtilityOps™ makes that the operational default.**

## NEXT STEPS

- 1 Request a platform demonstration
- 2 Review the module activation framework
- 3 Assess your highest-priority risk domains
- 4 Engage on a Phase 1 scoping conversation

