****

**White Paper:**

**How Seraphim Could Have Prevented the PG&E Wildfire Disaster**

**Executive Summary**

The catastrophic PG&E wildfires in 2018 and 2020 were among the most expensive and deadly infrastructure failures in U.S. history. Despite the presence of advanced telemetry and predictive analytics, PG&E failed to prevent these disasters due to systemic breakdowns in data interpretation, governance, and AI oversight. This white paper examines what went wrong at PG&E, what technology stack they relied on, and how Seraphim—a secure, auditable AI agent orchestration platform—would have fundamentally changed the outcome.

**Part I: What Happened at PG&E**

**Overview of the PG&E Wildfires**

* **2018 Camp Fire**: Sparked by a worn transmission line owned by PG&E, the Camp Fire killed 85 people and destroyed over 18,000 structures.
* **2020 Zogg Fire**: Another PG&E line ignited a wildfire that led to additional fatalities and mass evacuations.
* **Total Settlements**: PG&E paid over $13.5 billion in damages and was forced into bankruptcy.

**The Failure Points**

1. **Aging Infrastructure**: PG&E had extensive aging electrical infrastructure that required risk prioritization for repairs.

2. **Telemetry Systems**: They used sensor-based telemetry systems to monitor transmission lines for faults, pressure, and external factors like wind.

3. **Predictive Modeling**: PG&E employed third-party risk analytics and machine learning models to forecast where wildfires might occur.

4. **Governance Gaps**:

o No cross-validation between asset risk, weather data, and maintenance schedules.

o No escalation or override logic when certain risk thresholds were breached.

o No audit trail on AI decisions or outputs.

**Technology Stack (Approximate)**

* **Sensor Network**: IoT sensors attached to transmission lines and substations.
* **Data Ingestion**: SCADA systems and edge data streaming.
* **Analytics**: Custom-built risk models using statistical inference and machine learning.
* **Cloud Infrastructure**: AWS for data storage and compute.
* **Visualization**: Internal dashboards and geospatial mapping tools.

**What They Had:** Data + Models + Alerts  
 **What They Lacked:** Oversight + Integrity Checks + Governed Execution

**Part II: Introducing Seraphim**

Seraphim is an agentic AI orchestration platform designed to operate safely in regulated, high-risk environments. It provides the core control infrastructure missing from legacy AI deployments like PG&E's.

**Core Capabilities of Seraphim**

| **Pillar** | **Capability** | **Business Value** |
| --- | --- | --- |
| **Security** | Air-gapped or hybrid execution, agent sandboxing, human-in-the-loop approvals | Prevents unauthorized or unsupervised agent actions in critical infrastructure environments |
| **Integrity** | Cross-domain data validation, policy enforcement, business rule mapping | Ensures that incomplete, anomalous, or conflicting data is flagged and resolved before action |
| **Accuracy** | Real-time audit trail, IV&V modules, agent rollback | Guarantees traceability and allows decisions to be verified, challenged, and explained |

**Complementary Technical Modules**

* **Inspector Module**: Validates input/output data for completeness and compliance.
* **Conductor Module**: Coordinates AI agents across legacy and modern systems.
* **Controls Layer**: Applies RAG (retrieval-augmented generation) filters, policy constraints, and escalation logic.
* **Security Layer**: Supervises execution, prevents rogue automation, and supports full rollback.

**Part III: A Seraphim Scenario at PG&E**

Let’s reimagine the 2018 Camp Fire scenario with Seraphim in place.

**Step-by-Step Risk Mitigation**

| **Step** | **Without Seraphim** | **With Seraphim** |
| --- | --- | --- |
| **1. Data Ingestion** | Sensor data streamed from towers but not cross-referenced | **Integrity Layer** detects outdated maintenance logs and correlates wind risk |
| **2. Risk Modeling** | AI flags risk as "moderate" based on partial data | **Accuracy Layer** overrides risk classification due to contextual data gap |
| **3. Decision Execution** | No escalation or action taken before line failure | **Controls Layer** triggers immediate shutdown + dispatch agent escalation |
| **4. Governance** | No audit trail on decision or model logic | **Full audit trail** shows timestamped logic chain, model version, override justification |
| **5. Post-Incident Review** | No accountability, no root cause traceability | **Inspector Module** output is presented to legal, regulators, and board as evidence of compliance attempts |

**Part IV: Business & Operational Process Interventions**

Below is a decomposition of PG&E’s business and operational processes, and how Seraphim would have been a difference-maker at critical stages.

**Business Process Flow (Pre-Disaster)**

1. **Asset Management and Maintenance Scheduling**

o *Pain Point*: Missed inspections and outdated logs on aging infrastructure.

o *Seraphim Impact*: **Integrity Layer flags maintenance mismatches and escalates for action.**

2. **Risk Assessment and Weather Monitoring**

o *Pain Point*: No systemic integration between predictive weather models and asset criticality.

o *Seraphim Impact*: **Conductor Module fuses weather data with asset data in real-time.**

3. **Decision Making and Escalation**

o *Pain Point*: No human-in-the-loop logic or shutdown triggers despite risk thresholds.

o *Seraphim Impact*: **Controls Layer enforces policies, triggers shutdown protocols, and dispatches field agents.**

4. **Communication to Executives and Regulators**

o *Pain Point*: No defensible logic trail, model transparency, or internal alerts.

o *Seraphim Impact*: **Audit trail and inspector output provide executive dashboards and compliance reports.**

5. **Crisis Response and Liability Review**

o *Pain Point*: Legal exposure due to failure to act on data and internal warnings.

o *Seraphim Impact*: **Evidence of governed AI decisions, risk logs, and policy adherence reduces liability.**

**Part V: Business Outcomes with Seraphim**

**Quantifiable Prevention**

* **Avoided Losses**: $13.5B in settlements, lawsuits, and damage
* **Operational Continuity**: No bankruptcy, no grid loss
* **Governance Confidence**: Board and public stakeholders retain trust
* **Regulatory Standing**: Transparent audit trail reduces exposure to criminal liability

**Strategic Advantage**

* Compliance is embedded, not bolted on
* Auditability becomes a business asset, not a burden
* AI is deployed faster because risk is no longer a blocker

**Conclusion**

The PG&E disaster was not a failure of data or intent. It was a failure of **governance, traceability, and oversight** in AI-assisted infrastructure management. Seraphim is built specifically to address these gaps—making it the platform that not only enables enterprise AI adoption, but does so **without risking lives, lawsuits, or the company itself.**

Had PG&E implemented Seraphim, the Camp Fire would have been averted.

Seraphim isn’t just a platform. It’s the difference between operational AI—and operational catastrophe.

A logo with a flame and wings

AI-generated content may be incorrect.