LogZilla for Energy and Utilities

NERC CIP Compliance, Smart Grid Security, and SCADA Visibility

NERC CIP	SCADA	Zero	AI
Compliance Ready	Log Collection	Grid Impact	Copilot Included

The Energy Sector Challenge

Critical Infrastructure Protection:

- **NERC CIP compliance**: Mandatory audit requirements
- **Nation-state threats**: Grid is top target
- **OT/IT convergence**: SCADA meets enterprise
- **Smart grid complexity**: Millions of endpoints
- **Uptime requirements**: Grid cannot go down

The AI Advantage

Utility-Aware Intelligence:

- **NERC CIP automation**: Evidence generation
- **SCADA monitoring**: Passive, non-intrusive
- **APT detection**: Nation-state threat hunting
- **Smart meter security**: AMI visibility
- **Outage correlation**: Cyber-physical analysis

NERC CIP Compliance Coverage

Standard	Description	Status
CIP-003	Security Management Controls	Supports
CIP-004	Personnel & Training	Audit Trail
CIP-005	Electronic Security Perimeter	Monitoring
CIP-006	Physical Security	Log Collection
CIP-007	System Security Management	Supports
CIP-008	Incident Reporting	Automated
CIP-010	Configuration Management	Change Tracking
CIP-011	Information Protection	Access Logs

Audit-Ready: LogZilla provides the evidence collection and reporting required for NERC CIP audits and spot checks.

AI-Powered Grid Security

Grid Security Analyst prompt: "Analyze all SCADA and substation events for indicators of cyber attack in the last 24 hours."

```
GRID SECURITY ANALYSIS
Period: Last 24 Hours | Substations: 847 | Events: 124M
─────────────────────────────────────────
GRID STATUS: NORMAL (100% operational)

⚠ SECURITY ALERTS: 2

1. UNAUTHORIZED ACCESS ATTEMPT
   Target: Substation WEST-147 RTU | Protocol: DNP3
   Source: Unknown IP | Technique: Protocol fuzzing
   Status: BLOCKED - Firewall rule triggered

2. CONFIGURATION CHANGE DETECTED
   Device: EMS Server | Change: Firmware update
   User: admin_jsmith | Time: 02:14 AM
   Status: VERIFIED - Change ticket #4521

SCADA BASELINE: Normal 99.7% | Anomalous 0.3%
ASSETS: 23 plants ✓ | 124 substations ✓ | 700 feeders ✓
```

AI Use Cases for Utilities

Use Case	Traditional	With AI
NERC CIP audit evidence	Weeks	**Minutes**
APT threat detection	Days-Weeks	**Real-time**
SCADA anomaly analysis	Manual	**Automated**
Outage root cause	Hours	**Minutes**
Incident reporting	4-8 hours	**30 min**

OT Systems Supported

- **SCADA**: GE, Siemens, ABB, Schneider
- **EMS/DMS**: OSIsoft PI, AVEVA
- **RTUs**: SEL, GE, ABB
- **AMI**: Itron, Landis+Gyr, Sensus

Smart Grid and AMI Security

AMI Security Analyst prompt: "Analyze smart meter network for anomalies and potential tampering."

```
AMI SECURITY ANALYSIS
Period: Last 24 Hours | Meters: 2.4M | Events: 847M
═══════════════════════════════════════

FLEET HEALTH: 99.94% NORMAL

ANOMALIES DETECTED: 147

Meter Tampering Indicators:
  Physical tamper alerts: 23
  Magnetic interference: 12
  Reverse flow (no solar): 8
  → Field verification dispatched

Communication Anomalies:
  Unusual traffic patterns: 47
  Failed authentications: 34
  Protocol violations: 23
  → Firmware review scheduled

REVENUE PROTECTION:
  Estimated theft detected: $47,234
  Meters flagged: 43
  Investigations opened: 12

GRID EDGE SECURITY:
  DER (Solar/Battery): 12,341 monitored
  EV Chargers: 2,847 monitored
  Demand Response: 45,234 endpoints
```

Outage Correlation

```
OUTAGE ANALYSIS: SECTOR 47
Duration: 2h 14m | Customers: 12,341
═══════════════════════════════════════

ROOT CAUSE: Cyber-physical correlation

Timeline:
  14:21 - Firewall: Blocked scan attempt
  14:23 - SCADA: Unusual polling pattern
  14:24 - Substation: Breaker trip
  14:25 - OMS: Outage detected

DETERMINATION: Equipment failure
  (Cyber activity unrelated - coincidental)

Evidence preserved for NERC review
```

Regulatory Frameworks

Framework	Coverage
NERC CIP v7	Supports
NIST CSF	Supports
IEC 62351	Power Systems
IEEE 1686	Substation
TSA Pipeline	Oil & Gas

Deployment Options

On-Premises

- Control center
- Air-gap capable
- NERC CIP compliant
- Full data control

Regional

- Distributed collectors
- Central correlation
- Low latency
- Redundant paths

Hybrid

- OT data on-prem
- IT data in cloud
- Unified analytics
- Flexible architecture

Why Utilities Choose LogZilla

Metric	Improvement
NERC CIP audit prep	90% faster
Threat detection	Real-time
SCADA visibility	100% coverage
Incident response	85% faster

Utility-Specific Benefits:

- **Grid protection**: Zero operational impact
- **Compliance**: NERC CIP audit-ready
- **Visibility**: SCADA to smart meter
- **Resilience**: Cyber-physical correlation

Protect the grid, ensure compliance, maintain reliability.

sales@logzilla.net | www.logzilla.net