ABE POWERCOMM

INNOVATION - EXCELLENCE - INTEGRITY

We align power delivery and data networks to reduce risk, improve reliability, and modernize operations.

Risk and Gap Template for Electric Utilities

March 31, 2026

Summary

- This template is a structured tool for electric utilities to identify and address visibility gaps across the grid, communications network, facilities, and real-time operational status.

- It is designed to move beyond vague assessments by requiring each issue to be tied to a specific asset or process, the visibility needed, the current gap, the operational or business risk created by that gap, and the corrective action, owner, and timeline. The template uses scoring for likelihood, impact, and visibility maturity to prioritize risks and classify them as low, moderate, high, or critical.

- A typical assessment is organized into five main areas: grid visibility, network and communications visibility, facilities visibility, operational status and event visibility, and data quality and system integration. In this template we will focus on the network and communications visibility, facilities visibility, operational status and event visibility, data quality and system integration.

- For these areas, it provides key questions to ask, common risk scenarios, and a format to document findings. It also includes sections for sample risk statements, key performance indicators, and remediation roadmaps.

- Overall, the template helps utilities build a clearer picture of where they lack situational awareness, how those blind spots affect reliability, safety, restoration, cybersecurity, and compliance, and what actions are needed to improve visibility and operational readiness.

Objective

Assess risks and control gaps related to inadequate visibility across:

- Operational technology and communications networks
- Facilities and substations
- Real-time operational status, alarms, and events

Included Facilities:
Control Centers / Substations / Field Devices / AMI / SCADA / EMS / DMS / ADMS / Telecom & Data Networks / Physical Security

Stakeholders:
Operations, OT/SCADA, IT Network, Telecom, Field Operations, Substation Engineering, Cybersecurity, Asset Management, Compliance, Emergency Management

ABE POWERCOMM

Objective: What Good Looks Like

A mature utility visibility program should include:

1. Real-time visibility of critical grid state
2. Trusted asset and topology data
3. End-to-end OT communications monitoring
4. Integrated facility, environmental, and security visibility
5. Clear identification of stale data
6. A shared operating picture across control room, field operations, and network teams
7. Defined ownership for every major blind spot
8. Measurable KPIs and accountable remediation tracking

Without these capabilities, the utility does not have full situational awareness. It has fragmented awareness, which increases the chance of delayed response, poor decisions, preventable outages, and unmanaged operational risk.

ABE POWERCOMM

Risk Scoring Criteria

Likelihood Scale

1 – Rare: Unlikely to occur except in exceptional circumstances
2 – Unlikely: Could occur, but not expected frequently
3 – Possible: May occur under normal operating conditions
4 – Likely: Expected to occur periodically
5 – Almost Certain: Expected to occur frequently or repeatedly

Impact Scale

1 – Minimal: Little or no operational disruption
2 – Minor: Limited local disruption, manageable with routine response
3 – Moderate: Noticeable customer, operational, or service impact
4 – Major: Significant reliability, safety, regulatory, or operational impact
5 – Severe: Widespread or sustained service, safety, financial, or reputational impact

Visibility Maturity Scale

1 – None: No reliable visibility
2 – Limited: Partial, manual, or delayed visibility
3 – Basic: Some visibility, but major blind spots remain
4 – Managed: Good visibility with minor exceptions
5 – Mature: Comprehensive, near-real-time, trusted visibility

Risk Rating

Risk Score = Likelihood x Impact

1–5: Low
6–10: Moderate
11–15: High
16–25: Critical

ABE POWERCOMM

Risk and Gap Register

Example Entry

ID: R-001
Domain: Grid
Asset / Process: Distribution feeders
Visibility Requirement: Real-time feeder topology and breaker status
Current State: Partial SCADA coverage; some switching updates handled manually
Gap Description: Field switching is not consistently reflected in the network model
Risk Statement: If feeder topology is not updated in real time, operators may make switching decisions using an incorrect system state
Consequence: Extended outages, switching errors, safety exposure
Existing Controls: SCADA on major breakers, switching logs, operator confirmation calls
Likelihood: 4
Impact: 4
Risk Score: 16
Visibility Maturity: 2
Recommended Action: Expand telemetry and automate topology updates
Owner: DMS Manager
Target Date: [Insert date]
Status: Open

ABE POWERCOMM

A. Network and Communications Visibility

Network and Communications Visibility

Areas to Assess

1. OT network monitoring
2. WAN, LAN, radio, microwave, fiber, and cellular path visibility
3. Device health and availability
4. Latency, jitter, and packet loss monitoring
5. Redundancy and failover visibility
6. Router, switch, and firewall logging
7. Network segmentation visibility
8. Time synchronization monitoring
9. Third-party telecom dependency visibility

Key Questions

1. Can the utility tell whether a device is offline or just not reporting?
2. Is performance degradation monitored, or only total loss of communication?
3. Are communications issues correlated quickly to telemetry loss?
4. Are remote substations and field devices monitored at the same level as control centers?
5. Are unmanaged or legacy OT assets creating blind spots?

Typical Risks

1. Telemetry loss is mistaken for normal equipment status
2. Single points of telecom failure remain undetected
3. Network degradation delays operations or control actions
4. Poor logging delays cyber incident detection
5. Lack of OT observability hides lateral movement or abnormal traffic

ABE POWERCOMM

B. Facilities Visibility

Areas to Assess

1. Substation condition monitoring
2. Physical access and intrusion monitoring
3. Environmental monitoring, including temperature, smoke, flood, and fire
4. UPS, battery, and backup generator status
5. HVAC monitoring
6. Auxiliary system health
7. Video surveillance and remote alarm integration
8. Power supply status at unmanned sites

Key Questions

1. Are unmanned substations and remote sites visible in real time?
2. Can the utility detect environmental or auxiliary failures before they affect service?
3. Are physical security and environmental alarms integrated into operational monitoring?
4. Is backup power readiness visible and tested?

Typical Risks

1. Facility conditions worsen unnoticed until service is affected
2. Physical intrusion or tampering is not detected in time
3. HVAC or battery failures disable control equipment
4. Water, smoke, or fire damage escalates because alarms are isolated

C. Operational Status and Event Visibility

Areas to Assess

1. Alarm management
2. Event correlation
3. Sequence of events recording
4. Device health versus process health visibility
5. Data freshness and staleness monitoring
6. State estimation confidence
7. Network model accuracy
8. Operator dashboards and control room visibility
9. Incident escalation visibility
10. Restoration progress tracking

Key Questions

1. Are alarms rationalized, prioritized, and actionable?
2. Can operators clearly distinguish stale data from valid normal conditions?
3. Are major events automatically correlated, or manually interpreted?
4. Is there a common operating picture across control room, field operations, and network teams?
5. How quickly can leadership understand actual system status during a major event?

Typical Risks

1. Alarm floods hide real operational problems
2. Stale telemetry creates false confidence
3. Lack of common operating picture delays response
4. Manual reconciliation slows outage restoration
5. Weak event records limit post-incident analysis

D. Data Quality, Integration, and Governance

Areas to Assess

1. Data accuracy and completeness
2. Timestamp quality and time synchronization
3. Integration across SCADA, GIS, OMS, EMS, DMS, ADMS, AMI, and asset systems
4. Master asset identity consistency
5. Data latency
6. Missing telemetry rates
7. Exception handling
8. Ownership of data quality issues
9. KPI and KRI governance

Key Questions

1. Which system is the authoritative source for topology, status, and asset identity?
2. Are timestamps synchronized across systems?
3. Is bad or missing data measured and owned by a responsible team?
4. Are integrations real-time, near-real-time, or batch-based?
5. Is there a formal process to validate field changes against models and records?

Typical Risks

1. Operators act on inaccurate or stale data
2. Conflicting records create wrong dispatch or switching decisions
3. Lack of time sync weakens forensic analysis
4. No clear ownership causes recurring data quality failures

Example Risk Statements

1. Telemetry Blind Spots

If critical field devices do not provide reliable status and analog telemetry, the utility may be unable to detect abnormal system conditions early enough to prevent service disruption.

2. OT Network Observability

If the OT communications network lacks end-to-end monitoring, failures or degradation may be misclassified as equipment issues, delaying restoration and masking cyber or reliability events.

3. Facility Monitoring

If unmanned substations lack integrated environmental and security monitoring, physical or environmental conditions may go undetected until they impair operations or damage assets.

4. Data Freshness and Staleness

If stale telemetry is not clearly identified to operators, control-room decisions may be based on outdated information, causing unsafe or ineffective response actions.

5. System Integration

If SCADA, GIS, OMS, and ADMS views are not aligned, operators and field crews may act from conflicting versions of the system state, increasing outage duration and operational risk.

Key Performance Indicators and Key Risk Indicators

Metric	Definition	Current	Target	Threshold / Trigger	Owner
Telemetry Coverage %	Percentage of critical devices with real-time telemetry				
Status Accuracy %	Percentage of device states matching field reality				
Data Staleness Incidents	Count of stale or unflagged telemetry events				
Alarm Flood Events	Number of alarm storms above defined threshold				
Unmonitored Critical Sites	Count of critical sites without remote visibility				
Mean Time to Detect	Average time to detect loss of status or communications				
Mean Time to Restore Visibility	Average time to restore telemetry or monitoring				
Model Update Lag	Time between field change and system model update				

ABE POWERCOMM

Next Steps

Leadership Decisions Required

- Funding approval
- Scope prioritization
- Ownership and governance assignment
- Technology standardization
- Schedule commitment

Remediation Roadmap

Immediate Actions: 0–3 Months

1. Identify and address critical telemetry blind spots
2. Flag stale data clearly in operator displays
3. Inventory unmonitored critical assets and facilities
4. Rationalize top alarm overload issues
5. Validate top-priority network and facility dependencies

Near-Term Actions: 3–12 Months

1. Expand communications performance monitoring
2. Improve substation environmental and facility monitoring
3. Standardize asset identity, data ownership, and timestamps
4. Close major OT network monitoring gaps

Long-Term Actions: 12+ Months

1. Automate model and topology updates
2. Implement end-to-end OT observability
3. Develop predictive visibility analytics
4. Establish enterprise-wide common operating picture
5. Strengthen governance for ongoing visibility maturity improvement

ABE POWERCOMM

Closing

Turn visibility gaps into action. Engage us to assess where your data network, facilities, and operational status monitoring are exposing your utility to avoidable risk.

Dan Newman, PE, PENG
ABE PowerComm \\ Principal Consultant \\
daniel.newman@abepowercomm.com
http://linkedin.com/in/danielfnewman

ABE POWERCOMM