SCADA Audit Checklist for AI Readiness

10 things you need to check in your SCADA tags before you try to build a unified namespace

WorkSync | Operational Intelligence for Energy Infrastructure
work-sync.ai

Before You Build an Intelligence Layer

Most operators that invest in AI, predictive analytics, or operational intelligence platforms discover the same uncomfortable truth within the first 30 days: the technology works, but the data does not support it. Tag naming is inconsistent across RTUs. Historian data has gaps. Alarms fire so frequently that nobody pays attention. And nobody can map a SCADA tag to the actual asset it represents without asking the one technician who configured it eight years ago.

This checklist covers the 10 most common SCADA data quality issues that prevent AI and intelligence layer deployments from delivering value. Score each item honestly. The result will tell you exactly where to invest before you invest in AI.

Audit Item 1: Tag Naming Convention Consistency

What to Check: Are SCADA tags standardized across all RTUs, PLCs, and historians?

Why It Matters for AI: AI models require consistent identifiers to correlate data across assets. If Well_22_3_TBG_PSI and W223_TubingPress refer to the same measurement, the system cannot automatically build relationships.

Red Flags: Multiple naming conventions across vintages of equipment. Tags named by installer initials. No documented naming standard. Different formats for the same measurement type across areas.

Quick Win: Create a tag naming standard document. Map existing tags to the standard using an alias table. Most intelligence layers can handle aliases without requiring SCADA reconfiguration.

Score This Item:	[ ] 1 - Not Ready	[ ] 2 - Needs Work	[ ] 3 - AI-Ready

Audit Item 2: Data Polling Frequency Alignment

What to Check: Are critical tags polling at appropriate intervals for real-time analytics?

Why It Matters for AI: AI anomaly detection requires sufficient data resolution. A well producing 100 BOE/day being polled every 60 minutes will miss rapid pressure transients and rod pump failures that develop in minutes.

Red Flags: All tags polling at the same frequency regardless of criticality. High-value wells polling less frequently than low-value wells. No tiered polling strategy based on asset economics.

Quick Win: Implement a tiered polling strategy: critical production tags at 1-5 minute intervals, secondary monitoring at 15 minutes, status/environmental at 60 minutes.

Score This Item:	[ ] 1 - Not Ready	[ ] 2 - Needs Work	[ ] 3 - AI-Ready

Audit Item 3: Historian Data Quality

What to Check: What percentage of tags have gaps, flatlines, or stuck values in the last 90 days?

Why It Matters for AI: Machine learning models trained on data with gaps or stuck values will produce unreliable predictions. A pressure tag that reads 0 PSI for 72 hours because the RTU lost communication is not a data point. It is a data hole.

Red Flags: More than 5% of tags showing flatline values for 24+ hours. No automated data quality monitoring. Historian archiving silently dropping data points. No distinction between "zero production" and "communication failure."

Quick Win: Run a 90-day data quality audit. Flag all tags with gaps exceeding 4 hours. Implement quality codes to distinguish between real zero values and communication failures.

Score This Item:	[ ] 1 - Not Ready	[ ] 2 - Needs Work	[ ] 3 - AI-Ready

Audit Item 4: Alarm Rationalization Status

What to Check: How many alarms fire per day? What percentage are actionable vs. nuisance?

Why It Matters for AI: Alarm fatigue is the enemy of AI-driven exception management. If your SCADA system generates 500+ alarms per day and operators ignore 90% of them, an intelligence layer cannot distinguish signal from noise without first rationalizing the alarm configuration.

Red Flags: More than 10 alarms per operator per shift. Standing alarms that have been active for weeks. Alarms with no documented response procedure. Operators who have disabled or silenced alarm categories.

Quick Win: Conduct an ISA-18.2 alarm rationalization. Target fewer than 6 actionable alarms per operator per shift. Eliminate nuisance alarms. Document required response for every remaining alarm.

Score This Item:	[ ] 1 - Not Ready	[ ] 2 - Needs Work	[ ] 3 - AI-Ready

Audit Item 5: Tag-to-Asset Mapping Completeness

What to Check: Can every SCADA tag be mapped to a specific physical asset?

Why It Matters for AI: An intelligence layer needs to know that tag W223_TBG_PSI belongs to Well 22-3, which is in the North Area, operated by a specific crew, producing a specific commodity mix, with a specific lifting cost and decline profile. Without this mapping, data is just numbers.

Red Flags: Tags that nobody can identify without consulting the original installer. Orphaned tags from decommissioned wells still active in the historian. No single source mapping tags to API numbers or asset IDs.

Quick Win: Build a master tag-to-asset mapping table. Start with your top 20% of wells by production value. Cross-reference SCADA tags with production accounting well lists.

Score This Item:	[ ] 1 - Not Ready	[ ] 2 - Needs Work	[ ] 3 - AI-Ready

Audit Item 6: Multi-Vendor Normalization

What to Check: If you have multiple SCADA vendors, are data formats and units normalized?

Why It Matters for AI: Acquisitions, regional expansions, and technology refreshes create multi-vendor SCADA environments. ABB, Emerson, Honeywell, and other vendors use different data formats, timestamp conventions, and engineering units. An intelligence layer needs normalized, consistent data.

Red Flags: Different vendors using different engineering units for the same measurement. Timestamp discrepancies across systems. Duplicate well data in multiple historians with conflicting values.

Quick Win: Create a normalization specification document defining standard units, timestamp format (UTC recommended), and data quality codes across all vendors.

Score This Item:	[ ] 1 - Not Ready	[ ] 2 - Needs Work	[ ] 3 - AI-Ready

Audit Item 7: Communication Protocol Inventory

What to Check: What protocols are in use and which support publish/subscribe patterns?

Why It Matters for AI: Modern intelligence layers prefer publish/subscribe architectures (MQTT, OPC UA Pub/Sub) over legacy poll/response (Modbus, DNP3). Pub/sub enables real-time data streaming to the intelligence layer without additional load on the control system.

Red Flags: Reliance on legacy Modbus or DNP3 with no OPC UA gateway. No MQTT broker deployed. Data extraction requiring proprietary vendor tools. No documented protocol inventory.

Quick Win: Deploy an OPC UA gateway at the historian level. This provides standardized read-only access without touching field devices. Most major SCADA vendors support OPC UA server functionality.

Score This Item:	[ ] 1 - Not Ready	[ ] 2 - Needs Work	[ ] 3 - AI-Ready

Audit Item 8: Data Retention and Archival Policy

What to Check: How long is historian data retained and is it accessible via API?

Why It Matters for AI: AI models improve with historical depth. Predictive maintenance models need 12-24 months of history. Decline curve validation needs 3-5 years. If historical data is archived to tape or locked behind proprietary interfaces, your intelligence layer cannot access it.

Red Flags: Historical data older than 12 months archived offline. No API access to historian data. Data accessible only through vendor-specific client applications. No documented retention policy.

Quick Win: Ensure at minimum 24 months of high-resolution data is accessible via API. Implement a retention policy: 24 months at full resolution, 5 years at hourly averages, 10 years at daily summaries.

Score This Item:	[ ] 1 - Not Ready	[ ] 2 - Needs Work	[ ] 3 - AI-Ready

Audit Item 9: Cybersecurity Posture

What to Check: Are OT networks properly segmented with a DMZ for data extraction?

Why It Matters for AI: An intelligence layer needs to read data from OT systems. This requires a secure, well-architected DMZ (demilitarized zone) that allows data to flow from OT to IT without exposing control systems to external network access.

Red Flags: No network segmentation between IT and OT. Data extraction requiring direct connection to control system networks. No documented OT cybersecurity policy. No IEC 62443 or NIST framework compliance.

Quick Win: Implement a data diode or one-way gateway at the OT/IT boundary. Deploy the OPC UA gateway in the DMZ. Ensure the intelligence layer only reads from the DMZ, never from the control network directly.

Score This Item:	[ ] 1 - Not Ready	[ ] 2 - Needs Work	[ ] 3 - AI-Ready

Audit Item 10: Integration Readiness

What to Check: Does your SCADA system support read-only API access for external layers?

Why It Matters for AI: The most common deployment blocker is not technology. It is the six-month IT approval process required to grant API access to an external system. Understanding your integration readiness and starting the approval process early prevents delays.

Red Flags: No existing API integrations with external systems. IT/OT team unfamiliar with REST API or OPC UA client configuration. Change management process requiring 90+ days for new system integrations.

Quick Win: Start the IT/OT approval process in Phase 1, not Phase 2. Request read-only API access to historian data as the first integration step. Document the approval workflow and timeline.

Score This Item:	[ ] 1 - Not Ready	[ ] 2 - Needs Work	[ ] 3 - AI-Ready

Scoring Summary

Total your scores across all 10 items:

Score Range	AI Readiness Level	What It Means
10-15	Not Ready	Significant data foundation work needed before deploying AI or intelligence layers. Focus on tag standardization, data quality, and integration infrastructure.
16-22	Needs Work	Core infrastructure exists but gaps will limit AI effectiveness. Address the highest-priority red flags identified, then proceed with a scoped pilot.
23-30	AI-Ready	Your SCADA infrastructure can support an intelligence layer deployment. Proceed with integration and expect measurable results within 90 days.

Your Total Score: _____ / 30

Want a Detailed SCADA Integration Assessment?

WorkSync's engineering team can evaluate your SCADA infrastructure, identify integration points, and deliver a detailed readiness report in under a week. No cost. No commitment. Just clarity on where you stand.

Schedule an assessment: work-sync.ai/contact