Turning OT Data into Operational Advantage

How GILT bridges the gap between operational technology systems and actionable intelligence

The OT Data Landscape

Operational Technology environments generate and consume data at every layer of the control hierarchy — from field instruments and PLCs through SCADA/DCS systems to historians, MES platforms and enterprise integration layers. This data drives real-time control and safety decisions, but its value extends far beyond the control room.

Historian archives contain decades of process behaviour — millions of data points per day capturing temperatures, pressures, flows, levels, compositions, equipment states and alarm events. SCADA alarm logs reveal patterns in equipment reliability and operator response. DCS configurations encode the design intent of control strategies, interlock logic and safety functions. OT network topologies define the security boundaries that protect physical processes from cyber threats. Yet this data is rarely leveraged systematically because it sits in proprietary formats across disconnected systems with no unified way to query, correlate or analyse across boundaries.

The result is an enormous operational data estate that is rich in information but poor in accessible insight. The data exists to answer almost any operational question — but extracting those answers requires manual effort across multiple platforms, often by specialists who understand each system's proprietary interface.

How GILT Assists OT Professionals

- **Historian intelligence** — Direct API connectors to major historian platforms including OSIsoft PI, Honeywell PHD, Yokogawa Exaquantum and generic OPC-UA/OPC-DA interfaces. Time-series data is ingested with configurable resolution (raw, 1-minute, hourly averages) and aligned to the equipment entities identified in engineering documentation. This linkage means you can query process data in the context of the physical asset: "Show me the suction pressure trend for P-3201 over the last 6 months and flag any anomalies against the design operating envelope." The answer includes the trend data, the design parameters from the datasheet and any maintenance events that may correlate.
- **SCADA and alarm analytics** — Alarm event logs are parsed from DCS alarm journals or dedicated alarm management systems, deduplicated to remove chattering, and linked to equipment tags and their full documentation context. Identify standing alarms, alarm flood patterns, nuisance alarms and first-out trip sequences. Alarm data is not just listed — it is contextualised against the equipment, the process conditions at the time, and the historical pattern. Query: "What were the top 20 most frequent alarms in Area 400 last month and which equipment are they associated with?"
- **DCS configuration management** — Ingest and structure DCS configurations including control module definitions, interlock logic, setpoints, tuning parameters and I/O assignments. Compare as-built logic against design documentation to identify discrepancies. Track configuration changes over time to maintain a clear audit trail of modifications. Query: "Has the high-high trip setpoint for LT-4201 been changed from the original design value?"
- **OT network visibility** — Switch configurations, firewall rulesets and asset inventories are combined to provide a continuously updated view of the OT network topology, logical segmentation, zone and conduit compliance (per IEC 62443) and security posture. Configuration drift is detected automatically between baseline snapshots. Device firmware versions are cross-referenced against CVE databases for contextual vulnerability assessment.
- **Predictive maintenance** — Continuous analysis of process data against equipment performance baselines detects early signs of degradation. Heat exchanger fouling is tracked through UA trending. Compressor efficiency drift is monitored against design curves. Pump performance deviation flags bearing or impeller issues. Control valve stiction and hysteresis are identified from process variable and controller output patterns. Early detection shifts maintenance from reactive to predictive, reducing unplanned downtime and extending asset life.

Supported Platforms & Protocols

GILT integrates with the major OT platforms and protocols deployed across heavy industry:

- **Historians** — OSIsoft PI (PI AF, PI Data Archive), Honeywell PHD, Yokogawa Exaquantum, GE Proficy, AVEVA Historian, Canary Labs, InfluxDB and generic OPC-UA/OPC-DA interfaces. Time-series data is ingested at configurable resolution and aligned to engineering documentation.
- **SCADA/DCS** — Honeywell Experion, Emerson DeltaV, ABB 800xA, Yokogawa CENTUM VP, Siemens PCS 7, Schneider EcoStruxure, Citect, Ignition and WinCC. Configuration data, alarm journals, event logs and batch records are all supported.
- **Network Infrastructure** — Cisco IE/Catalyst, Hirschmann, Siemens SCALANCE, Belden, Moxa. Firewalls from Palo Alto, Fortinet, Cisco ASA, Hirschmann EAGLE and Tofino. Configuration exports are parsed and structured automatically.
- **CMMS** — SAP PM, IBM Maximo, Infor EAM and similar platforms. Work orders, defect notifications, PM schedules and spare parts records are ingested and linked to equipment entities.

Integration, Not Replacement

GILT does not replace existing OT systems — it works alongside what you already have. Connections to historians, SCADA, DCS and network infrastructure use standard interfaces and secure, read-only protocols. There is no rip-and-replace, no 18-month implementation programme, and no disruption to existing operations. GILT deploys alongside your existing infrastructure and starts delivering value from your existing data within weeks. As new data arrives — new documents, updated configurations, additional historian tags — the knowledge base grows incrementally without requiring a full rebuild. The intelligence layer compounds over time: the more data GILT ingests, the richer the cross-references and the more powerful the insights become.

Automated Reporting & Dashboards

GILT generates structured outputs tailored to OT stakeholders. Equipment health dashboards aggregate historian trends, alarm data and maintenance history into a single view with drill-down to source data. Shift handover reports are generated automatically, summarising key events, alarm activity and equipment status changes. Compliance registers track regulatory obligations with automated scheduling. Configuration audit reports document DCS and network changes with full before/after comparison. All outputs integrate with Excel, PowerBI, web dashboards and API endpoints.

Security Posture

OT data is treated with the highest sensitivity classification. The architecture respects IEC 62443 zone and conduit segmentation principles. All data is encrypted in transit (TLS 1.3) and at rest (AES-256) with per-client key management backed by hardware security modules. Processing environments are logically isolated per client with no cross-client data access. OT network configurations are processed in dedicated, isolated compute instances and are never stored in shared environments. Role-based access with MFA ensures least privilege. All access events are logged with tamper-evident audit trails. GILT does not retain client data or IP beyond the engagement — all data is securely deleted with cryptographic verification.