Smarter Control Systems Start with Smarter Data

How GILT helps controls engineers access, query and act on plant data faster

The Controls Engineer's Data Problem

Controls engineers work across SCADA/DCS platforms, historian data, alarm management systems, cause-and-effect diagrams, loop drawings, SIS documentation and vendor manuals on a daily basis. The challenge is rarely a lack of data — it's that the data lives in disconnected systems with no unified way to query across them.

When a control loop behaves unexpectedly, you're switching between the historian, the DCS configuration, the C&E diagram and the original datasheet to piece together what's happening. When a safety instrumented function needs review, you're cross-referencing HAZOP nodes, SIL verification reports, proof test records and maintenance history manually. When an alarm rationalisation study is required, you're exporting alarm logs, manually categorising thousands of events and trying to link them back to equipment context.

This fragmentation costs time, introduces error and means that critical context is often missed. GILT eliminates this problem by creating a unified, queryable knowledge layer across all of your control system data.

How GILT Assists Controls Engineers

- **Loop-level intelligence** — Query any control loop and get its full context in a single response: P&ID location, C&E logic, setpoints, alarm settings, tuning parameters (gain, integral, derivative), historian trends and maintenance events. Every piece of information is linked to its source document with page and revision traceability. Ask "What are the current alarm setpoints for FIC-4201 and when were they last changed?" and get an immediate, sourced answer.
- **Alarm rationalisation support** — GILT ingests alarm event logs from your DCS or alarm management platform, deduplicates chattering alarms, identifies standing alarms and alarm flood patterns, and links every alarm point to its equipment tag and associated documentation. Systematic identification of nuisance alarms and rationalisation opportunities replaces manual spreadsheet analysis. Query: "Which alarms in Area 200 have activated more than 50 times in the last 30 days?"
- **SIS and SIL documentation** — Cross-reference safety instrumented functions against their HAZOP basis, SIL target determination, SIL verification calculations (PFDavg), proof test procedures, proof test records and maintenance history. Instantly answer questions like "When was SIF-4201 last proof tested, what was the result, and when is the next test due?" GILT maintains the full traceability chain from hazard identification through to proof test compliance.
- **First-out trip analysis** — When a plant trips, GILT automatically interrogates trip sequence data, alarm event logs and process historian trends to reconstruct the event timeline and identify the most probable initiating cause. The system correlates first-out signals with upstream process conditions, cross-references equipment documentation and presents a structured root-cause analysis — reducing diagnosis time from hours to minutes.
- **C&E and logic verification** — Query cause-and-effect relationships across your facility. Compare DCS logic implementations against design intent documentation to identify discrepancies. Ask "Show me the C&E logic for compressor K-4201 shutdown" and get the complete cause-and-effect matrix with source references.
- **Control narrative access** — Retrieve control narratives, functional descriptions and operating procedures for any control loop or system. When troubleshooting unfamiliar equipment or reviewing legacy systems, GILT provides instant access to the original design intent alongside current configuration.

Integration with Existing Control Platforms

GILT connects to your existing infrastructure through standard interfaces — no rip-and-replace required. Direct API connectors to major historian platforms (OSIsoft PI, Honeywell PHD, Yokogawa Exaquantum, OPC-UA/DA) enable time-series ingestion at configurable resolution. DCS configurations, alarm journals and event logs are ingested from Honeywell Experion, Emerson DeltaV, ABB 800xA, Yokogawa CENTUM and Siemens PCS 7 environments. SCADA data from platforms including Citect, Ignition and WinCC is supported. GILT operates as a read-only intelligence layer alongside your existing systems, delivering value from existing data within weeks of deployment — not months.

Impact for Controls Teams

- Diagnosis time for plant trips reduced from hours to minutes through automated first-out analysis and event correlation
- Alarm rationalisation studies completed in days rather than weeks, with systematic rather than manual categorisation
- SIS compliance tracking automated with full audit trail from HAZOP basis through to proof test records
- Control loop troubleshooting accelerated by providing complete loop context in a single query
- Legacy system knowledge preserved and accessible even after original engineers have moved on
- Reduced reliance on individual expertise — the knowledge is in the system, not just in people's heads
- MOC (Management of Change) support — when changes are proposed, GILT identifies all affected loops, interlocks and safety functions

How It Works — The Technical Foundation

GILT's knowledge architecture is specifically designed for the cross-referencing demands of control system data. Rather than treating documents as flat text, GILT builds a multi-layer knowledge graph where every entity — every loop, every tag, every alarm point — is a node connected to all of its related documentation, configuration data and operational history. When you query a control loop, the system traverses this graph to assemble complete context from across all source systems in milliseconds. Domain-adapted embedding models ensure that control system terminology (PFDavg, BPCS, ESD, MOS, TIF) is interpreted with engineering precision rather than generic language model approximation. Every response includes full provenance — document name, page, revision — so you can verify any answer against its source.

Security You Can Trust

GILT handles OT and control system data with the highest sensitivity classification. The architecture is informed by 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. Processing environments are logically isolated per client with no cross-client data access by design. Role-based access control with multi-factor authentication ensures principle of least privilege. All access events are logged with tamper-evident audit trails. GILT does not retain client data or IP beyond the engagement period — all data, including embeddings, vector indices and knowledge graph contents, is securely deleted upon project completion with cryptographic verification. For Australian clients, all processing occurs on Australian-hosted infrastructure. GILT never connects directly to live control systems — it operates as a read-only intelligence layer ingesting data through secure, controlled transfer processes.

© 2026 GILT. All rights reserved. | Confidential