



SERVICE SPECIFICATION / OPERATIONAL SYSTEMS

Operational automation and integration

GHT-SVC-030 · Revision 1.0 · 06 September 2026 · 1 / 3

Supported APIs, webhooks, files, records, alerts, approvals, schedules, and devices connect with validation, limited permissions, duplicate protection, logs, retries, and manual recovery.

Intended outcome

A tested automated process that records each state, flags incomplete work, prevents duplicate effects, and can be paused, retried, reversed, or completed manually.

Service scope

Automation can connect APIs, webhooks, files, databases, message queues, notifications, schedules, identity platforms, and physical devices. The workflow needs a source of truth, schema, permissions, timing, validation, duplicate handling, error states, audit log, and owner.

Physical or safety-related actions deserve stricter boundaries than informational updates. A system should fail to a documented state and preserve a manual path rather than silently fabricating success or repeatedly issuing an unsafe command.

How the system fits together

01 Trigger	Event, schedule, threshold, user action, approved device state
02 Decision	Validation, policy, authorization, approval, idempotency, state
03 Action	API, webhook, message, record, notification, device or human task
04 Evidence	Audit, status, acknowledgement, exception, retry, rollback, manual close

Typical project triggers

- Staff copy the same data between systems or repeatedly chase the same status
- Alerts lack routing, acknowledgement, escalation, or closure evidence
- An existing script depends on one person, shared credentials, or invisible scheduled tasks
- Duplicate, delayed, partial, or failed workflows cannot be traced and resolved



GHT-SVC-030 / OPERATIONAL AUTOMATION AND INTEGRATION

Delivery and acceptance

Revision 1.0 · 06 September 2026 · 2 / 3

The final project scope identifies quantities, locations, dependencies, and the evidence required at each delivery stage.

01 Observe and bound the work

Map trigger, actors, systems, data, decisions, approvals, timing, exceptions, volume, current evidence, and cost of failure.

Acceptance evidence: Current-state sequence, sample records, rule inventory, exception categories, owner, and success metric.

02 Design the control path

Define source of truth, schema, validation, least privilege, approval, idempotency, retry, timeout, logging, alerts, rollback, retention, and manual fallback.

Acceptance evidence: Future-state sequence, data contract, permission and secret-owner model, failure table, and acceptance cases.

03 Build and release progressively

Use test data and constrained accounts, log every transition, protect credentials, stage read-only or approval modes where useful, and release to a limited group.

Acceptance evidence: Versioned configuration, test records, audit events, deployment record, rollback method, and pilot results.

04 Attack the assumptions

Test duplicate, stale, missing, malformed, unauthorized, delayed, out-of-order, rate-limited, unavailable, partially completed, rollback, and manual completion cases.

Acceptance evidence: Acceptance results, alert and audit samples, resolved exceptions, recovery time observations, and owner runbook.

Handover deliverables

- Current- and future-state workflow diagrams
- Data contract, field mapping, rules, permissions, and owner matrix
- Failure-mode, retry, rollback, reconciliation, and manual-fallback design
- Normal, exception, security, load-bound, and recovery acceptance evidence
- Version, monitoring, change, credential-owner, and operator runbook

Closeout: GHT and the customer review the agreed evidence, record unresolved exceptions and owners, and confirm acceptance against the signed project scope.



GHT-SVC-030 / OPERATIONAL AUTOMATION AND INTEGRATION

Planning and scope boundaries

Revision 1.0 · 06 September 2026 · 3 / 3

Customer and site inputs

- Trigger, owner, frequency, volume, timing, business rule, and completion evidence
- Systems of record, supported interfaces, schemas, identifiers, and data quality
- Authentication, authorization, approvals, credential owner, rate limits, and retention
- Duplicate, stale, missing, failed, partial, timeout, retry, rollback, and manual paths
- Change windows, monitoring, alert routing, support ownership, test data, and acceptance metrics

Constraints and coordination

- Automation is limited by source-data quality, interface support, rate limits, licensing, and platform change
- Credentials and service accounts require protected storage, least privilege, rotation, and named ownership; secret values should never appear in documentation
- Automated external, financial, safety, or physical actions may require human approval and additional controls
- A workflow can be technically available while producing an incorrect business result; outcome reconciliation remains necessary

Commercial scope and responsibilities

This specification describes the service framework. The signed statement of work defines included equipment, quantities, software licenses, integrations, access windows, schedule, pricing, warranty, and support coverage. Additional construction, electrical work, recurring subscriptions, and ongoing support require an explicit line item.

The customer appoints an acceptance owner and provides authorized access, required site information, and decisions. GHT records assumptions, coordinates assigned work, and submits changes for agreement before expanding the scope.

Technical references

National Institute of Standards and Technology — SP 800-128: Security-Focused Configuration Management | Source review: 2026-08-20

National Institute of Standards and Technology — SP 800-82 Rev. 3: Guide to Operational Technology Security | Source review: 2026-08-20

National Institute of Standards and Technology — SP 800-207: Zero Trust Architecture | Source review: 2026-08-20

Service guide and project discussion | Source review: 2026-09-06