SERVICE SPECIFICATION / OPERATIONAL SYSTEMS

Operational technology networks

GHT-SVC-032 • Revision 1.0 • 06 September 2026 • 1 / 3

Asset discovery, approved data paths, industrial switching, remote access, monitoring, backups, maintenance windows, testing, and rollback, all with process-owner approval.

Intended outcome

A current OT asset and communication map, tested network boundaries, approved remote access, recoverable configurations, and process-aware acceptance results.

Service scope

Operational technology includes programmable systems and devices that interact with the physical environment, such as industrial controls, building automation, transportation, utilities, physical access, and environmental monitoring. Their safety, timing, reliability, and availability needs can differ materially from office IT.

An OT project should begin with asset and data-flow discovery performed without disrupting production. Architecture, segmentation, monitoring, patching, remote access, backups, and incident response must be coordinated with process owners and equipment vendors.

How the system fits together

01 Process and assets	Controllers, sensors, actuators, HMIs, servers, building and physical systems
02 Zones and conduits	Criticality boundaries, industrial links, approved protocols and data paths
03 Controlled access	Identity, jump path, vendor session, least privilege, logging and approval
04 Operations and recovery	Monitoring, time, configuration backup, spares, change window, rollback and incident plan

Typical project triggers

- Controls, building systems, cameras, vendors, and office devices share a flat undocumented network
- Remote vendor access uses permanent shared credentials or unmanaged consumer hardware
- No one can produce current asset, firmware, network, backup, or communication-path records
- Changes are made without a process owner, maintenance window, backup, test, or rollback

Delivery and acceptance

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

01 Discover without disruption

Coordinate with process and safety owners; inventory assets, versions, protocols, dependencies, vendors, data flows, remote paths, network equipment, time, backups, and allowable methods.

Acceptance evidence: Owner-approved asset and communication inventory, current topology, criticality, maintenance constraints, and discovery limitations.

02 Design zones and controlled paths

Define security zones, conduits, industrial switching, routing, firewall policy, remote access, identity, logging, time, redundancy, monitoring, configuration backup, and recovery.

Acceptance evidence: Target architecture, approved communication matrix, access model, equipment and resilience schedule, backup plan, test plan, and rollback criteria.

03 Change in approved windows

Back up configurations, stage equipment, pretest rules, label connections, implement an approved segment at a time, observe process state, and retain a working rollback path.

Acceptance evidence: Pre-change backup checks, labeled assets and links, change log, owner observations, configuration record, and rollback readiness.

04 Validate process and recovery

Confirm approved communications, blocked paths, latency-sensitive functions, alarms, time, redundancy, monitoring, remote access, configuration restoration, and process-owner acceptance.

Acceptance evidence: Communication and segmentation test results, process acceptance, monitoring events, remote-access audit sample, restoration test, and exceptions.

Handover deliverables

- Approved OT asset, owner, version, criticality, and communication inventory
- Current and target zone/conduit architecture and policy matrix
- Remote-access, identity, monitoring, time, backup, change, and rollback design
- Communication, segmentation, process, monitoring, and restoration acceptance evidence
- Labeled as-builts, configuration archive, exception register, and operating runbook

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

Planning and scope boundaries

Customer and site inputs

- Process, safety, availability, timing, environmental, regulatory, and maintenance-window constraints
- Assets, firmware, protocols, addresses, criticality, owners, vendors, and lifecycle status
- Current and required data flows, zones, remote access, identity, time, logging, and monitoring
- Industrial media, distances, redundancy, enclosures, power, grounding, spares, and support
- Configuration backups, restore method, test environment, change approval, validation, rollback, and incident response

Constraints and coordination

- OT changes can affect safety, production, warranties, validated processes, and vendor support; process-owner approval is required
- Active discovery, vulnerability scanning, failover, patching, or restoration tests can disrupt fragile equipment and must be explicitly approved
- Legacy protocols and devices may lack modern authentication, encryption, logging, or patch paths
- Security improvements must preserve required deterministic behavior, local control, safe states, and recovery

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 800-82 Rev. 3: Guide to Operational Technology Security | Source review: 2026-08-20

International Society of Automation — ISA/IEC 62443 Series of Standards | Source review: 2026-08-20

Cybersecurity and Infrastructure Security Agency — Cross-Sector Cybersecurity Performance Goals | Source review: 2026-08-20

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