

SC CDM · HITL GATES · CONTROL TOWER · MCP AGENTS · EDI/WMS SANDBOX

AI Supply Chain & Logistics Control Tower

Dockerized AISC for ERP/WMS/TMS/carrier CDM ingest, risk & inventory intelligence, MCP exception agents, HITL PO/transfer gates, Control Tower UI, DOC/WH/SQL/eval, EDI/WMS sandbox sync, network-transfer verify, learning export, and cost/OBS — governed supply-chain ops AI that keeps humans on sensitive writes, not an ERP chatbot.

M0–M10
MILESTONES CLOSED

PASS
PHASE 1 / MVP / 3

1.0.0
API VERSION

PASS
SMOKE_M10

Built by **Abdul Basit** · AI Automation Engineer · Delivery closeout 2026-09-12

BUSINESS IMPACT

Fewer silent sync fails · safer SC writes · audit-ready logistics ops
Sources→CDM→agents→HITL→Control Tower · unauthorized 0 · approval 100% · silent writes 0 · Phase gates Met · ERP/WMS remain SoR

OVERVIEW

Logistics signals normalize into a shared CDM. FastAPI owns RAG, MCP allowlists, HITL, exceptions, DOC/WH/SQL/eval, EDI/WMS sandbox, learning, cost metering, and the Control Tower. n8n runs thin HTTP wrappers with a global DLQ. **ERP/WMS/TMS/carrier remain systems of record.** Auth is X-API-Key + X-RoIe on every write surface. Live OAuth/EDI VAN and production cutover are fixture/API-first with written waivers (**W-01**); Docker Compose sandbox is the agreed gate for acceptance.

TYPE	AI supply chain control tower (FastAPI + n8n; not a single Zap)
ROLE	AI Automation Engineer / Supply Chain Ops AI Engineer
USERS	SC Ops · Logistics · Planner · Buyer · Finance approver · Analyst · Platform admin
DELIVERY	API 1.0.0 · Milestone M10 · Closeout 2026-09-12 · Milestones doc v2.1
STACK	FastAPI · n8n · Postgres · Redis · Qdrant · MinIO · Caddy · Compose aisc
PORTS	API 8002 · n8n 5680 · Caddy 8082 · Qdrant 6335 · MinIO 9020
BUYERS	SC Ops / logistics teams needing gated, grounded automation with proof metrics

THE PROBLEM Signal sprawl — ERP/WMS/TMS/carrier never share a CDM Silent fails — sync errors look like success Ungoverned AI — PO/transfer without HITL Stock lag — reorder without audit trail Exception fog — no queue / resume path Analyst drift — invented ETAs / root causes No closeout — cannot prove gate metrics	THE SOLUTION FastAPI AISC — CDM, agents, HITL, SQL deny Thin n8n — ingest / notify / DLQ only MCP ACL — audited tool denies HITL gates — PO · transfer · escalate Control Tower — exceptions + KPIs + cost P1/P2 depth — DOC/WH/SQL · EDI/WMS · verify Kill switch — platform-wide write stop	WHO IT SERVES - Teams needing gated SC AI - Ops needing exception queues + SLA - Planners / buyers with PO HITL - Analysts with tool-bound Q&A - Admins with connectors + kill switch - Lead path: \$6.1 shipment → HITL - Secondary: EDI · transfer · SQL reject
--	---	---

CAPABILITY SURFACES

SURFACE	FOCUS	SURFACE	FOCUS
Ingest / CDM	ERP · WMS · TMS · carrier · EDI sandbox	Agents / MCP	Shipment · replenish · supplier · analyst
HITL / EXC	PO · transfer · escalate · assign/resume	Ops UI	/ops/ui/ · cost · aisc_* metrics
P1 depth	DOC · WH · SQL · SUP reply · eval	P2 depth	EDI · WMS net · transfer verify · learning · K8s

GATE METRICS (UAT SAMPLE)

METRIC	TARGET	RESULT	EVIDENCE
Unauthorized agent actions	0	0	mcp_deny_analyst_write · UAT
Approval compliance	100%	100%	HITL roles · sampled gates
Silent write failures	0	0	SQL reject · fail-closed paths
Closeout smoke	PASS	M10_SMOKE_OK	tests/smoke_m10.py · health 1.0.0

Lead journey: shipment investigate → exception → HITL → verify. **Secondary:** replenish HITL · SQL write reject · EDI/WMS sync · transfer verify. **Closeout:** smoke_m10 PASS · ACCEPTANCE Signed (sandbox).

Architecture rule: FastAPI owns AI / AuthZ / HITL / CDM · n8n stays thin · sensitive writes require approval · SQL writes rejected · ERP/WMS remain SoR · env-only secrets · live prod deferred W-01.

LAYERED ARCHITECTURE · GOLDEN PATHS · SAFETY PROOFS

Architecture, journeys, agents, and safety proofs

Principle: FastAPI owns agents, HITL, RAG, MCP, and CDM; **n8n owns thin side effects** — no god-workflow. Fail closed; never invent shipment/inventory facts.

```
Sources (ERP / WMS / TMS / carrier / EDI fixtures)
→ FastAPI ingest (normalize + idempotent upsert) + MinIO payloads/docs
→ Postgres CDM · Qdrant SC RAG · Redis kill-switch / rate limits
→ Agents/MCP allowlists · HITL (PO / transfer / escalate) · Exceptions
→ P1: documents / warehouse / SQL / eval / supplier reply
→ P2: EDI sync · WMS network · transfer verify · learning · K8s docs
→ Ops UI /cost /metrics (aisc_*) · n8n DLQ · smoke_m10
```

COMPONENT	ROLE IN THE SYSTEM
Ingest adapters	Source envelopes → CDM; fixture demos m2–m9; idempotent upsert; MinIO raw refs
Ops UI + API	/ops/ui/ ; Auth X-API-Key + X-RoLe; OpenAPI /docs; port 8002
MCP server	Per-agent allowlists; analyst cannot update_shipment / inventory_transfer
HITL / Approvals	PO_HITL_USD; inventory transfer always HITL + post-write verify
SQL gateway	Allowlisted SELECT only; DDL/DML → writes_and_ddl_rejected
Kill switch / cost	POST /admin/kill-switch; soft budget via /cost/summary
n8n catalog	wf_sc_ingest · shipment · inventory · PO · approval · reply · wf_error_global

INTELLIGENCE

- SC RAG + citations / no-invent escalate
- Shipment investigate + confidence gate
- Replenish recommend + PO HITL
- Supplier escalate + SUP-02 reply loop
- Text-to-SQL allowlisted SELECT only
- Eval scorecards + learning export
- Warehouse bottleneck insights

INTEGRATIONS

ERP / WMS / TMS	M2 fixture adapters
Carrier tracking	ETA / event fixtures
EDI PO confirm	/integrations/edi/sync
WMS network	/integrations/wms/*
Transfer verify	HITL + inventory_levels
Documents	BOL/invoice OCR stub
K8s / live prod	Docs / W-01 deferred

SAFETY & OPS

- HITL before PO / transfer / escalate
- SQL write reject audited
- MCP deny for analyst writes
- Kill switch + cost soft budget
- DLQ / fail-closed paths
- Idempotent CDM upserts
- Append-oriented audit_events

LEAD JOURNEYS (\$6.1–\$6.6)

- \$6.1 shipment investigate → exception → HITL → verify
- \$6.2 stockout → replenish recommend → PO HITL
- \$6.3 overdue PO escalate → approve → notify
- \$6.4 BOL/invoice ingest → mismatch exception
- \$6.5 analyst tool-grounded Q&A (no free SQL)
- \$6.6 low-confidence → queue (no invented root cause)
- Extras: EDI/WMS sync · network transfer verify

SECURITY PROOF POINTS

Missing/invalid API key blocked. Analyst MCP write denied. SQL DELETE → writes_and_ddl_rejected. Transfer without approval blocked; post-approve path verifies inventory. Kill switch stops agent writes. UAT: unauthorized **0** · approval **100%** · silent writes **0**.

- Approver roles: sc_ops_manager · planner · buyer · finance
- Evidence: docs/m10/samples/uat_results.json

```
Reproduce: docker compose up -d --build · curl :8002/health (1.0.0) · docker compose exec -T api python -m tests.smoke_m1 → M10_SMOKE_OK · UI /ops/ui/
```

Demo arc: shipment→HITL→Control Tower primary · SQL deny / EDI / transfer secondary · cite health **1.0.0** · closeout smoke PASS · ACCEPTANCE Signed (sandbox).

Reliability, full milestone unlock, Phase gates, closeout

RELIABILITY AND SC SAFETY

AREA	WHAT SHIPPED
Auth	X-API-Key + X-RoLe (sc_ops / planner / buyer / finance / admin...)
MCP	Per-agent allowlists · audited denies · analyst write deny
HITL	Approve before PO / transfer / escalate send
SQL	Allowlisted SELECT · reject DDL/DML + audit
Verify	Transfer mutates + verifies inventory_levels
Kill switch	POST /admin/kill-switch blocks agent writes
Cost	Soft budget alerts via /cost + OBS aisc_*
Idempotency	Duplicate events → no duplicate side effects
Audit	Agent runs · approvals · tool denies · integrations

PHASE GATES + CLOSEOUT

- **Phase 1 (M4)** — CDM; risk/inventory; MCP; confidence escalate; unauthorized → **0**
- **MVP / Phase 2 (M7)** — \$6.1–\$6.3/\$6.6; P0 n8n; HITL; Control Tower; silent fails → **0**
- **Phase 3 (M10)** — DOC/WH/SQL/eval; EDI/WMS/learning; docs+KT; sandbox Met; live **W-01**

MILESTONE UNLOCK (M0–M10)

M0–M1	Architecture · Compose · RBAC · audit · kill-switch
M2–M3	CDM connectors · risk · replenish · RAG citations
M4–M5	MCP · exceptions · HITL · analyst · escalate
M6–M7	n8n E2E · Control Tower · MVP gate Signed
M8–M9	DOC/WH/SQL/eval · EDI/WMS · transfer · learning
M10	UAT · cutover · KT · ACCEPTANCE · API 1.0.0

CLOSEOUT SMOKE EVIDENCE (UAT_RESULTS.JSON)

CHECK	RESULT	PROVES
health_1_0_0	true	aisc-api 1.0.0 + postgres/redis/qdrant/minio healthy
mcp_deny_analyst_write	true	Analyst denied update_shipment / inventory_transfer
sql_write_reject	true	DELETE → writes_and_ddl_rejected
hitl_approver_roles	true	sc_ops_manager / planner in APPROVER_ROLES
unauthorized_zero / approval_100 / silent_zero	true	Phase 3 gate metrics
m10_docs_present	true	OPS-05 closeout pack present

N8N P0 CATALOG

- wf_sc_ingest · wf_shipment_event
- wf_inventory_monitor · wf_po_supplier_monitor
- wf_exception_action · wf_approval / notify
- wf_supplier_reply · wf_error_global

DAY-2 RUNBOOK (FIRST ACTIONS)

- Exception backlog → assign / resolve with reason
- Approvals queue → decide with approver role
- Connector unhealthy → re-sync EDI/WMS sandbox
- DLQ depth → inspect dead letters · redrive
- Unsafe agent → enable kill switch · audit · disable

SCOPE HONESTY · BUYER FAQ · HOW TO RUN · ACCEPTANCE

What this is, what it is not, and how to reproduce

IN SCOPE (DELIVERED)

- Full M0–M10 on Docker Compose (API 1.0.0)
- CDM connectors + EDI/WMS sandbox sync
- MCP exception agents + HITL approvals
- Control Tower UI + cost/OBS (aisc_*)
- DOC/WH/SQL/eval + supplier reply loop
- Network transfer HITL + inventory verify
- Learning → eval export + K8s sample manifests
- UAT Pass + ACCEPTANCE Signed (sandbox)
- KT pack + cutover checklist + runbooks

DEFERRED / WAIVED

- Live production cutover / DNS/TLS/IdP (**W-01**)
- Live ERP/WMS/TMS/carrier OAuth
- Live EDI AS2/VAN network
- SMS/voice alert channels (m8)
- Next.js apps/web/ (static UI delivered)
- Online model fine-tune (out of scope)
- Live cluster apply for K8s samples
- Client wet-signature UAT workshop

BUYER FAQ

QUESTION	HONEST ANSWER
System of record?	ERP / WMS / TMS / carrier remain SoR. AISC normalizes into a CDM for ops AI; it does not replace the ledger or WMS.
EDI / OAuth live?	Sandbox / fixtures for UAT and acceptance. Live credentials and EDI VAN waived until provided.
What does acceptance prove?	CDM, MCP deny, HITL, SQL reject, transfer verify, smoke_m10 PASS at API 1.0.0 — not live OTIF uplift claims.
Live production included?	No — cutover waived (W-01). Sandbox Compose acceptance is the contracted-equivalent gate.
Agents create POs alone?	No — PO / transfer / escalate require HITL; unauthorized MCP writes denied and audited.
Where is evidence?	docs/m0–m10, smoke_m10, ACCEPTANCE, REQUIREMENTS_CHECKLIST, uat_results.json.

REPRODUCE (SUMMARY)

```
cd "12-AI Supply Chain & Logistics Control Tower"
docker compose up -d --build
curl http://localhost:8002/health # version 1.0.0
docker compose exec -T api python -m tests.smoke_m10 # M10_SMOKE_OK
docker compose exec -T -e PYTHONPATH=/app api pytest tests/test_m10_closeout.py -q
open http://localhost:8002/ops/ui/ + http://localhost:8002/docs
```

ACCEPTANCE OUTCOMES

- Unauthorized agent actions: **0**
- Approval compliance (sample): **100%**
- Silent write failures: **0**
- Phase 1 / MVP / Phase 3: **Met**
- UAT: **Pass** (fixture attestation)
- ACCEPTANCE: **Signed / Met** (sandbox)

PACK & UPLOAD

- Pack: flagship portfolios/12-AI Supply Chain.../
- Paste kit: UPWORK_UPLOAD.md
- Setup: SETUP.md · Loom: LOOM_SCRIPT.md
- Gallery: architecture PNG · before/after · PDF
- Rebuild: python assets/write_svgs.py · render_exports.py

One-liner: AISC — Dockerized FastAPI + n8n supply chain control tower with CDM, MCP HITL, Control Tower, DOC/SQL/eval, EDI/WMS sandbox, transfer verify — M0–M10 complete at API 1.0.0.

This is: a closed M0–M10 supply-chain control tower with governed agents and sandbox acceptance. **This is not:** an ERP/WMS replacement, unsupervised inventory automation, or a completed live production cutover.

VISUAL EVIDENCE

Architecture diagram and before → after panel

