

PROJECT 042 - AI AGENT + TOOLS + HUMAN APPROVAL SYSTEM

Portfolio Case Study | AI Operations Agent • PostgreSQL • Slack • Human-in-the-Loop • Audit Logging

Executive Summary
Project 042 is an AI-powered operations system designed to let users query business data naturally while preventing the AI from making sensitive database changes without explicit human authorization. The system combines an n8n AI Agent, PostgreSQL tools, conversation memory, Slack approval controls, validation logic, and a persistent audit trail. Read operations can be handled autonomously; write operations are converted into pending approval requests and executed only after a verified human decision.

1. Business Problem

AI agents are useful for operational work because they can interpret natural-language requests and decide which tools to use. The risk appears when the same agent is allowed to directly modify production data. A misunderstood instruction, hallucinated value, duplicate request, or accidental execution could change an order or another business record without oversight.

This project addresses that control gap. The design separates information retrieval from state-changing actions. The AI may inspect orders, customers, and operational information, but an order-status update is treated as a protected action that must pass through a human approval workflow.

2. Solution Architecture

Workflow 01 - Main AI Operations Agent	Workflow 02 - Human Approval & Order Update
Receives a natural-language request, reasons over the request, uses the appropriate PostgreSQL tool, maintains conversation context, and creates an approval request when a protected write operation is requested.	Validates the pending approval, sends an interactive Slack approval card, receives the human decision, re-validates the record, routes Approve/Reject, performs the authorized action, sends confirmation, and writes the outcome to the audit log.

3. Core Components

- AI Operations Agent: Interprets user intent and selects the correct operational tool instead of relying on a single rigid workflow path.
- AI Reasoning Model: Provides the language understanding and tool-selection capability used by the agent.
- Conversation Memory: Preserves conversational context so follow-up requests can be understood within the active session.
- Order Lookup: Reads order records and current order status from PostgreSQL.
- Customer Lookup: Retrieves customer information when the request requires customer-level context.
- Operations Intelligence: Supports broader operational queries and structured business-data retrieval.
- Request Human Approval: Creates a pending approval record rather than directly changing protected order data.

4. Human-in-the-Loop Control Design

The key design principle is that AI intent is not equivalent to authorization. When a user requests a protected order update, Workflow 01 first retrieves the current record and creates a unique approval request. The response explicitly reports the current status, requested new status, approval ID, and Pending state while confirming that the order itself has not yet been modified.

Workflow 02 then retrieves that approval record and validates that it is still pending before creating the Slack approval card. After a human clicks Approve or Reject, the workflow retrieves the approval again and checks its current state before routing the decision. This second validation reduces the risk of stale, duplicate, or previously processed decisions being executed.

5. Controlled Execution Paths

APPROVED PATH

Receive Human Decision → Parse Approval Decision → Retrieve Approval Request → Validate Still Pending → Route Approval Decision → Approve & Update Order → Send Approval Confirmation → Log Approved Action

REJECTED PATH

Receive Human Decision → Parse Approval Decision → Retrieve Approval Request → Validate Still Pending → Route Approval Decision → Reject Request → Send Rejection Confirmation → Log Rejected Action

6. End-to-End Testing

The system was tested with real workflow executions using sample order records. A representative test requested a change for ORD-1051 from Processing to Ready for Dispatch. Workflow 01 correctly created approval APR-DECC9DC5 with a Pending status and did not modify the order before authorization.

- Read-only test: The agent successfully retrieved an order's current status using the Order Lookup tool.
- Approval creation test: A requested write operation produced a pending approval instead of an immediate database update.
- Slack approval test: The approval request was surfaced as an interactive card containing the approval ID, order ID, requested status, requested action, and Approve/Reject controls.
- Approved-path test: The authorized branch updated the order, sent a Slack confirmation, and wrote an Approved audit record.
- Rejected-path test: The rejection branch prevented the requested order change, sent a rejection confirmation, and logged the rejected action.
- Audit verification: Audit output captured fields such as request ID, user request, intent, tool used, target ID, approval requirement, approval status, execution result, agent response, and timestamp.

7. Reliability & Safety Controls

Control	Purpose
Read/write separation	Allows autonomous retrieval while protecting state-changing operations.
Unique approval IDs	Provides traceability between the AI request, Slack decision, execution, and audit record.
Pending-state validation	Prevents an already resolved approval from being treated as a fresh request.
Decision routing	Ensures only the approved branch reaches the order-update query.
Human authorization	Keeps a person in control of consequential database changes.
Persistent audit logging	Creates evidence of what was requested, authorized, executed, and reported.

8. Business Value

The architecture demonstrates how an SMB can introduce AI into operational workflows without giving the model unrestricted control over business data. Employees gain a conversational interface for retrieving information and initiating actions, while management retains an approval checkpoint for consequential changes. The result is a practical balance between automation speed, human accountability, database integrity, and traceability.

9. Technology Stack & Skills Demonstrated

Platform	n8n self-hosted automation environment
AI	AI Agent architecture, LLM reasoning, tool selection, conversation memory
Database	PostgreSQL queries, order/customer retrieval, approval records, controlled updates, audit logging
Human approval	Slack interactive approval workflow with Approve/Reject routing
Engineering concepts	Human-in-the-loop, validation, protected writes, deterministic execution, state management, traceability

Project Outcome

A tested two-workflow AI operations system capable of autonomous business-data retrieval and controlled order updates through human authorization. Both approval and rejection paths were validated, confirmations were delivered through Slack, and execution outcomes were captured in PostgreSQL audit records.