**Claude Breakdown: Chunk 1 — System Overview + Core Architecture**

**✅ Scope**

Define the foundational architecture of ClubOS V2:

* Action-based, mobile-first operator interface
* Single-LLM agent per deployment
* Modular routing to tools (Claude, OpenPhone, NinjaOne, DB, etc.)
* No chatbot behavior — action-only logic, no multi-turn conversational flow
* Starts human-in-loop, builds toward autonomous trust via feedback loops

**🔁 Cross-Referenced Corrections**

| **Early Plan** | **Final Decision** |
| --- | --- |
| 4 LLMs (tech, booking, etc.) | ✅ Single unified LLM per instance |
| Static SOP logic | ✅ AI-monitored, human-approved updates |
| Human escalation always manual | ✅ Escalation logic is toggle-configurable |

**🔧 Dependencies**

* OpenAI or Claude runtime w/ tool call support
* Railway + Vercel deployment stack (Node backend, Next.js frontend)
* NinjaOne, Ubiquiti, Skedda or Jason’s booking API, OpenPhone
* Claude (or equivalent) for file parsing + SOP injection

**📋 Tasks**

**[1.1] Set System Identity and Mode**

* Default LLM agent name: OperatorGPT
* Only one agent per deployment
* Must be able to:
  + Take customer messages
  + Route action requests (reset, unlock, etc.)
  + Search + invoke SOP logic
  + Call Claude for SOP parsing or feedback review

**[1.2] Define LLM Autonomy Profile (per action type)**

{

"tech": { "autonomy": true, "max\_fallbacks": 1 },

"booking": { "autonomy": false },

"access": { "autonomy": true, "rules": ["within 10 min of booking", "no flags"] },

"faq": { "autonomy": true }

}

**[1.3] Implement Control Toggles**

* Each autonomy behavior is controlled by:
  + Action category
  + Booking metadata
  + Confidence score
* Fallback logic is not hardcoded — defined in config

**[1.4] Claude Role**

* Claude is only used for:
  + SOP file ingestion
  + Conflict detection
  + Knowledge merge suggestions
  + Flagged feedback loop processing
* All Claude edits are flagged for human approval

**✅ Expected Behavior**

* System starts with **OperatorGPT** receiving all inbound messages
* No other assistants are used
* Based on message intent and context, the LLM:
  + Executes actions
  + Escalates if configured to
  + Logs all outcomes
* Claude only invoked when:
  + New knowledge is uploaded
  + SOPs need review or cleanup
  + Human requests change

proceed to **Chunk 2: Message Flow, Thread State, and Escalation Logic**.