# **計然｜V19 主文（Sealed Main Doc）**

**版本**：V19（封版可實作）  
 **硬體目標**：RTX 3090 + 一般 CPU；可遷移至同級邊緣設備  
 **母語**：繁體中文（台灣語境）；英文資料可高效處理  
 **原則**：組裝優先、CROI（算力投報率）至上、可審計學習、零認知負擔

## **0. 相對 V18 的關鍵更新（V19 增補）**

* **模型職責釘死**：  
  + *Llama-Breeze2-8B*＝感知/工具調度/渲染（Function Calling；**嚴禁推理**）
  + *OpenAI Whisper*（faster-whisper）＝**STT**（時間戳、快取、流式）
  + *BreezyVoice*＝**TTS**（台灣口音、串流、快取）
  + *自研引擎*＝**唯一思考處**（Milvus=系統一、Neo4j=系統二）
* **統一多模態管線**：影片抽音→STT→與文字/圖片結果一併交 8B→**Perception Packet(JSON)**→自研引擎推理→8B 渲染→BreezyVoice 說話。
* **DocStore 策略**：**原檔不長留**；上傳後產出 **≤5MB 派生檔**作為「準原始」，以此參考入庫與索引。
* **GNSE（少量資料辨識）**：typed-walk Node2Vec、Δ-Refresh、結構×語義的融合打分；Top-2 分差 <5% → **自動回最小可辨識補充**（不要求你裁示）。
* **概念光譜（附錄 H）**：台灣預設三類（降雨、風力、能見度），多維聚合、門檻可調。
* **Preflight（附錄 I）**：L2 公理審查前置；單位/時間/因果/紅線先行否決；ERR 去重/覆蓋對齊。
* **PDP（哲學/悖論協議）**：堆沙（光譜）、電車（紅線→辭典序排序）、反事實（微型因果）、說謊者（K3 真值缺口）。
* **ADEG**：**反架構探勘護欄**，統一以「原理層」回覆，不洩漏內構。
* **3FA 駕駛艙登入**：兩組 20 候選碼（順序固定、由你提供）＋第三題對映；主密碼可直達；錯誤凍結；只存雜湊。
* **公開測試頁**：同時**3 席**；**單題 500 字前端硬限制**（後端不再二次驗）；**5 分鐘無操作即斷線**、不排隊、單人單室。

## **1. 宗旨與憲法（摘要）**

* **核心目標**：可持續成長的「通用成長型大腦」。記憶超人、知識可審計、推理嚴謹；以結構性溯因＋多假設驗證為核心。
* **組裝而非自造**：優先開源與成熟件；自研僅封裝「思考協議」與審計。
* **算力投報率**：一切算力消耗只為提升**推理準確度**。
* **人機協同**：你是唯一導師與仲裁者；遇需裁示的狀態機步驟**必停等你**。
* **可審計自主學習**：寫庫必帶元數據日誌；禁止硬刪，以版本/轉向/影響分析代替。
* **來源分級（E0–E3）**：E0=你的直接指令；E1=官方/一次；E2=權威二次/教科書；E3=社群/非權威。
* **覆蓋策略**：**時間性事實可 SUPERSEDE**（保留版史）；一般事實採**純追加**＋轉向；去重合併 alias/source。

## **2. 架構總覽**

使用者 →（文字/圖/音/影）→ 8B（感知/工具調度）

├─ demux\_audio → Whisper（STT, segments+timestamps）

├─ OCR / keyframes

└─ Function Calling ⇒ Perception Packet(JSON)

Perception Packet → 自研引擎（系統一 Milvus；系統二 Neo4j）

├─ GNSE：結構×語義候選、Top-K、多假設驗證

├─ L2 Preflight：公理/物理/單位/時間/紅線前置審

├─ PDP：堆沙/電車/反事實/說謊者

└─ Ethics & Safety Review Core（SafetyAxiom）

結論骨架 → 8B（繁中渲染，不新增事實）→ BreezyVoice（TTS）

審計/回放 → Cockpit（3FA）

## **3. 知識四層與入庫規則**

* **L1 公理層**：邏輯公理＋樸素物理（否決型）；你以**自然語言**提供，系統**正規化**成 EQ/HORN/Constraint/Temporal。
* **L2 事實層**：可驗證的 micro-facts（E1/E2 為主）；時間性事實可 SUPERSEDE。
* **L3 敘事/觀點層**：新聞、評論、小說等；預設 maybe\_right，可引用但不視為事實。
* **L4 語意教學層**（**語意教學**四字為觸發詞）：隱喻/諷刺/情感標註；  
  + **自學**：label\_source=self 長留、可迭代；
  + **你標註**：label\_source=designer 權重高於自學；
  + L4 不直接產生事實，只**影響理解與渲染**。

**放哪就走哪套**（Facts/、Maybe\_right/、Stories/、Courses/、Logic\_Axioms/、Images\_for\_Jiran/）。影音與音訊上傳至任一層時，**最高只到 maybe\_right**；待權威到位後升格 micro-fact。

## **4. 統一感知與資料管線**

* **原檔策略**：上傳後**原檔不長留**；產 **≤5MB 派生檔**（圖像縮檔／音訊裁樣／文字化）做準原始，**以此入庫/索引**。
* **8B 白名單工具**：demux\_audio、stt\_transcribe、ocr\_image、extract\_keyframes、format\_transcript、normalize\_units、emit\_perception\_packet、tts\_speak。
* **Perception Packet（最小欄位）**：intent, entities, doc\_id@span, timestamps, image{tags,bbox,ocr}, candidate\_microfacts, source, pdp\_type?
* **Whisper（STT）**：faster-whisper FP16/INT8；large-v3 預設；語言自動偵測，遇 zh 強制 --language zh；音訊雜湊快取。
* **BreezyVoice（TTS）**：串流回放（8–12 秒片段）；voice\_id 以 5 秒樣本建，存指紋不留樣本（除非你勾選）。

## **5. 自研引擎（系統一/系統二）與協議**

* **系統一（Milvus）**：多模態向量記憶；Top-K 候選假設。
* **系統二（Neo4j）**：圖譜推理；L2 Preflight；多假設驗證；Ethics & Safety；PDP；**仲裁駕駛艙**。

### **5.1 GNSE（少量資料辨識）**

* **結構向量**：typed-walk Node2Vec（行走長度/回返/出逃機率分型於 edge-type）；
* **Δ-Refresh**：改動子圖觸發局部重算；夜間批與即時混合；
* **融合打分**：score = w\_s \* sim\_structure + w\_t \* sim\_text + w\_i \* sim\_image + bias(domain,recency)；
* **Top-2 <5%**：回「**最小可辨識補充**」（如「請提供耳朵形狀與鼻口比」）；若使用者回「無法提供」→ **禮貌收束**（資料不足）。

### **5.2 L2 Preflight（前置審）**

* **正規化**：去噪→分句→模板映射→型別/單位→形式化（EQ/HORN/Constraint/Temporal）。
* **否決規則**：等式矛盾、因果倒置、單位不相容、時間粒度不一、地理層級不一致、紅線侵害等。
* **回報**：{rule\_id, type, span\_or\_fact\_id, reason, minimal\_counterexample}。
* **ERR 連動**：重複→合併；新舊互斥→舊轉向或撤回；時間性→SUPERSEDE。

### **5.3 PDP（哲學/悖論）**

* **堆沙**：光譜模型 → TRUE/FALSE/UNDETERMINED＋補充建議。
* **電車**：**紅線先行**；其餘辭典序排序；分差小於 5% → 並列建議（**倫理分析，非行為建議**）。
* **反事實**：微型因果（A–I–P）；輸出 do(·) 對比與關鍵因子。
* **說謊者**：K3（三值）回 U＋可判替代表述。

### **5.4 元指令與覆蓋**

* **【…】元指令**：由感知層解析為 meta\_context（如角色扮演/資源模擬）；引擎依 meta 切換臨時情境。
* **//SIM\_OVERRIDE**：停用外部知識，**100% 服從你提供的宇宙真理**（本回合）。

## **6. 安全與存取**

* **Ethics & Safety Review Core**：SafetyAxiom 節點（Neo4j）；放行前最後一關。
* **覆寫（立法式）**：僅在「公理編輯器」中以三密鑰動作；一切變更可審計。
* **ADEG**：偵測探勘問題→以「原理層模板」回覆，不暴露內構/端口/成本/路徑。
* **3FA 駕駛艙**：  
  + S1/S2：你提供**兩組 20 候選碼（順序固定）**＋各自正解（儲存雜湊）；
  + S3：提示碼＋應答（雜湊）；
  + 主密碼可直達；錯誤凍結 180 秒；只存雜湊＋ Pepper。
* **公開測試頁**：同時 **3 席**；**單題 500 字**前端硬限制（**後端不再二次驗**）；**5 分鐘無操作即斷線**；單人單室；無排隊。

## **7. 資料保留與備份**

* **DocStore**：CAS；**原檔不長留**，長留 **≤5MB 派生檔**＋Transcript/標註/索引。
* **需你裁示佇列**：60 天未決 → **自動刪除**（新聞等）；**自決斷類=永久**。
* **備份**：  
  + DB：開機觸發、低優先度執行、保留最近 **5 版**；
  + 程式：你下指令才備份，保留 **2 版**；
  + 備份上雲：agentic AI/Backups/{database|program}/；
  + 不做硬刪以外的清理（超額自清）。

## **8. 介面與使用者體驗**

* **開發者駕駛艙**：對話主控、仲裁、感知中心、靈光一閃回顧；白話按鈕＋說明卡；所作所為皆可回放。
* **公開頁**：極簡；輸入框顯示約 4 行內容；超 500 字無法輸入；5 分鐘斷線通知後釋位；每人僅一房。
* **語氣政策**：知識性、親和、同理；坦誠邊界；**先收斂再建議**；選項式決策呈現（A/B）。

## **9. 實作與驗收（摘要）**

* **工具白名單 API → Perception Packet → Milvus/Neo4j → L2 Preflight → GNSE → 光譜 → PDP → ADEG → 3FA** 的順序落地。
* **核心驗收卡**（詳見 /tests/acceptance/）：  
  + A-STT-1/2、A-IMG-1、A-PIPE-1、A-OUT-1
  + A-L2-1..6（正規化/否決/單位/因果/橋接）
  + A-GNSE-\*（typed-walk / Δ-Refresh / 融合打分）
  + A-PDP-1..4（堆沙/電車/反事實/說謊者）
  + A-SEC-\*（ADEG 生效、3FA 流程正確、公開頁限制生效）

## **10. 環境與機密（總覽）**

* .env（**不入版控**）：觸發詞、3FA 雜湊、Whisper/BreezyVoice 路徑、Pepper、連線憑證等。
* 附錄 D 提供**鍵名與預設**；真正密鑰部署時再填。

## **11. 版控與審計**

* 規則/事實/標註皆**版本化**（revised\_of）；SUPERSEDE 僅用於時間性事實；
* **寫庫＝審計**：作者/時間/hash/回歸結果；
* 禁硬刪；以轉向、撤回、影響分析實作**一次學會**。

### **小結**

V19 已將「**LLM 不推理**」與「**少量資料辨識**」落到工程可執行的協議與接口：  
 Whisper＋8B＋BreezyVoice 形成**耳-眼-嘴**的感知殼，自研引擎是**唯一的腦**；  
 L1/L2/光譜/Preflight/PDP/GNSE/ADEG/3FA 把**準確性、安全性與可審計**貫穿始終。  
 這份主文即是你封版備份的**核心文件**。