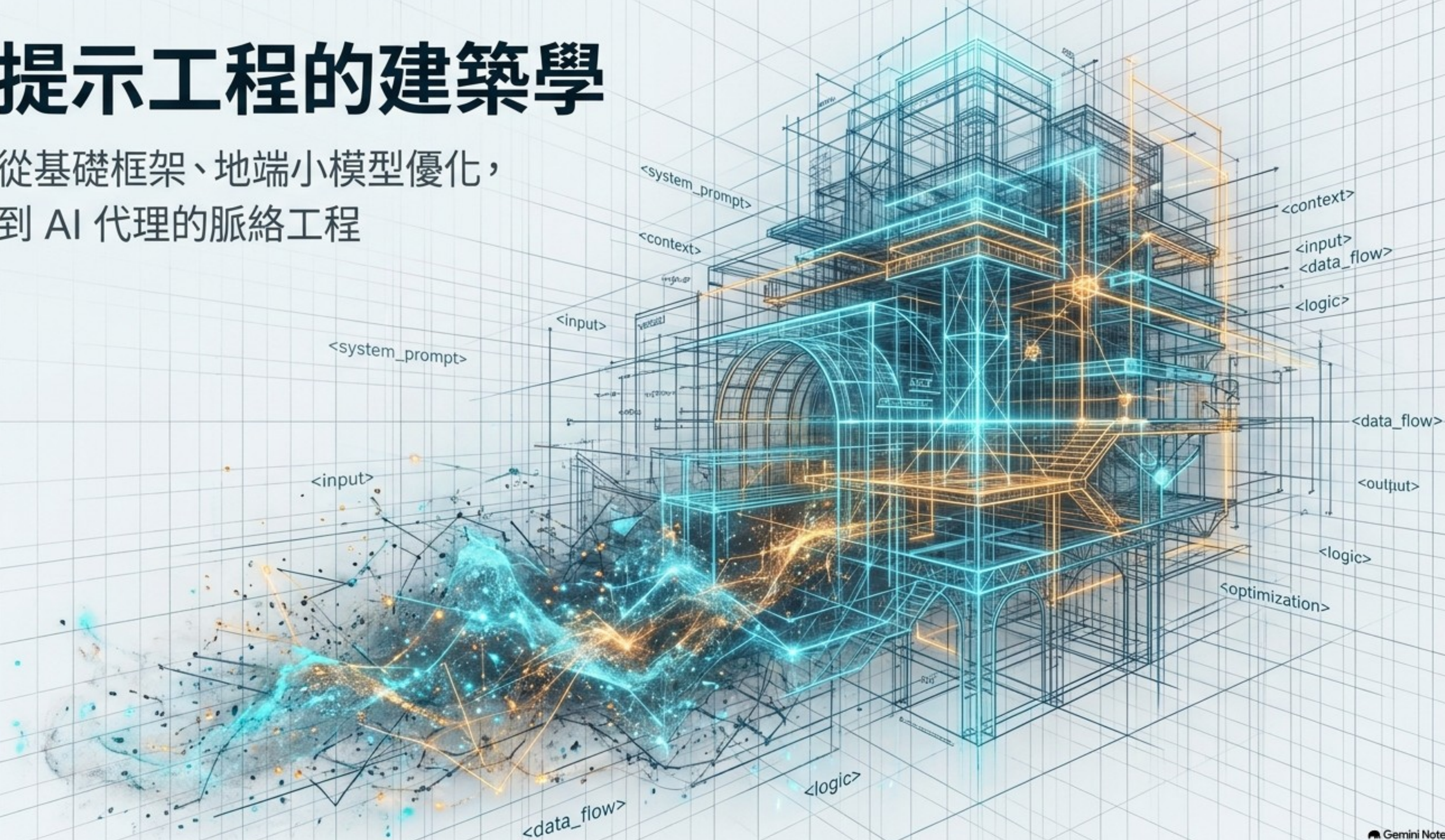


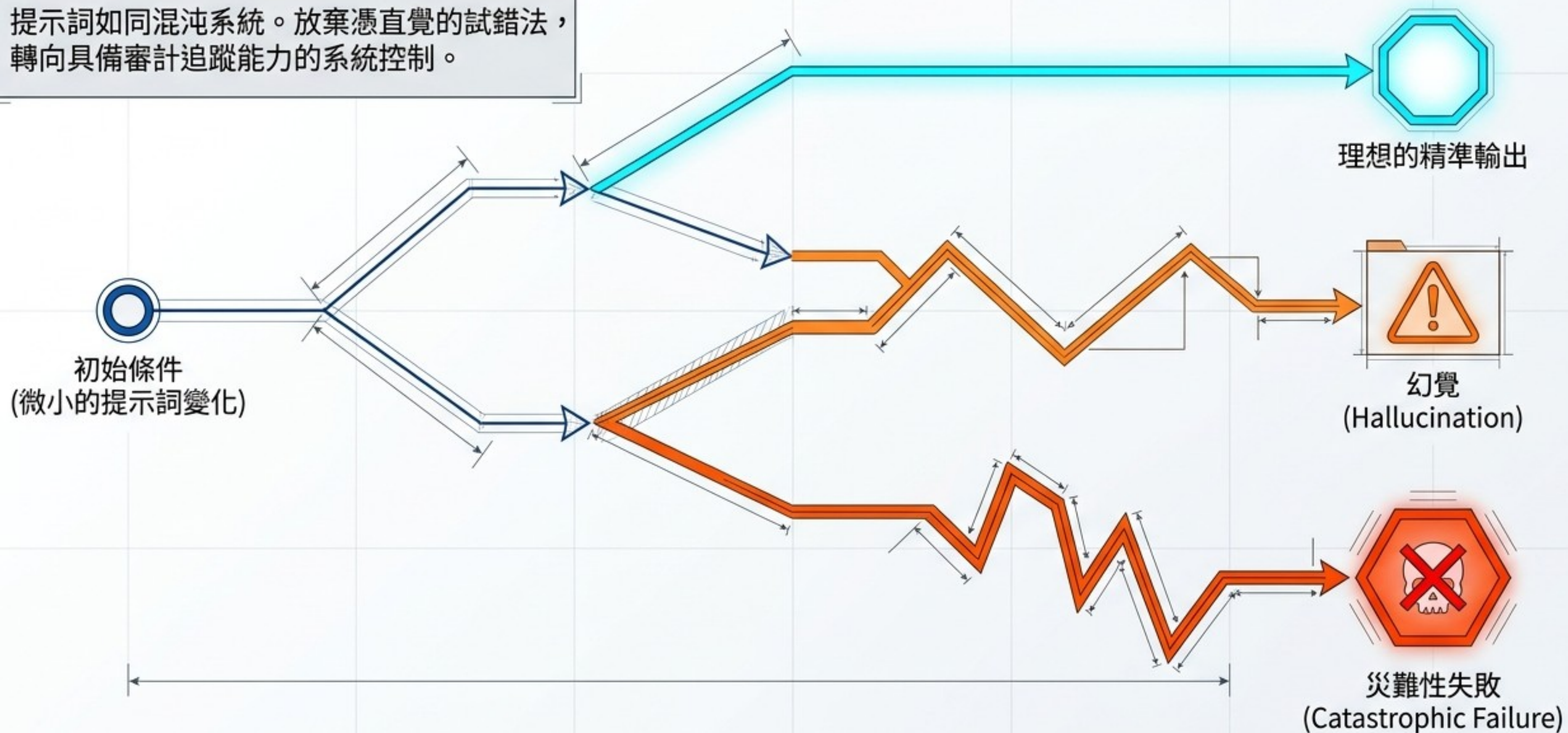
提示工程的建築學

從基礎框架、地端小模型優化，
到 AI 代理的脈絡工程



初始條件問題：自然語言的蝴蝶效應

提示詞如同混沌系統。放棄憑直覺的試錯法，
轉向具備審計追蹤能力的系統控制。



從工藝到工程：AI 控制學的演進

Level 3 : 脈絡工程 (Context Engineering)

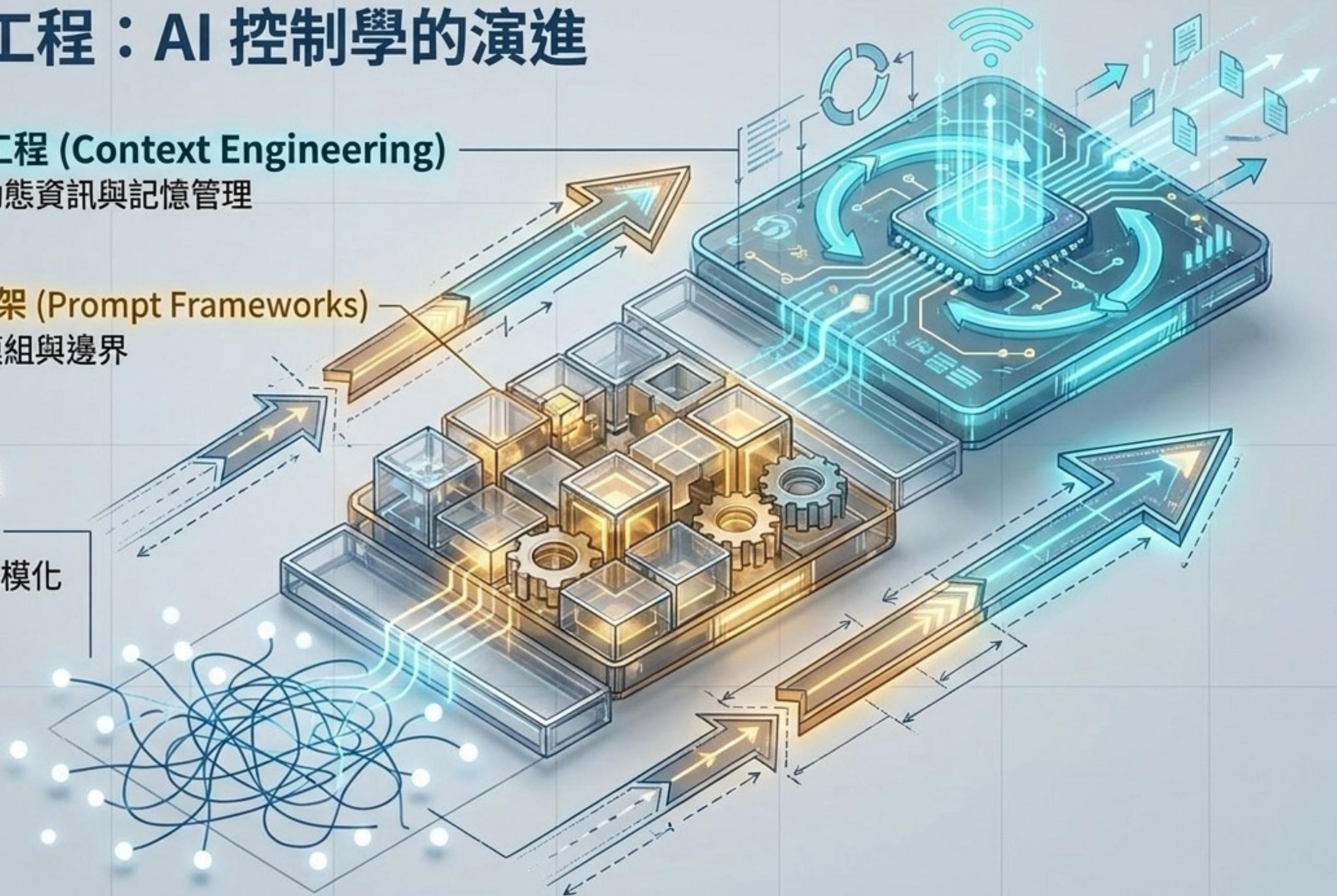
針對自主代理的動態資訊與記憶管理

Level 2 : 提示框架 (Prompt Frameworks)

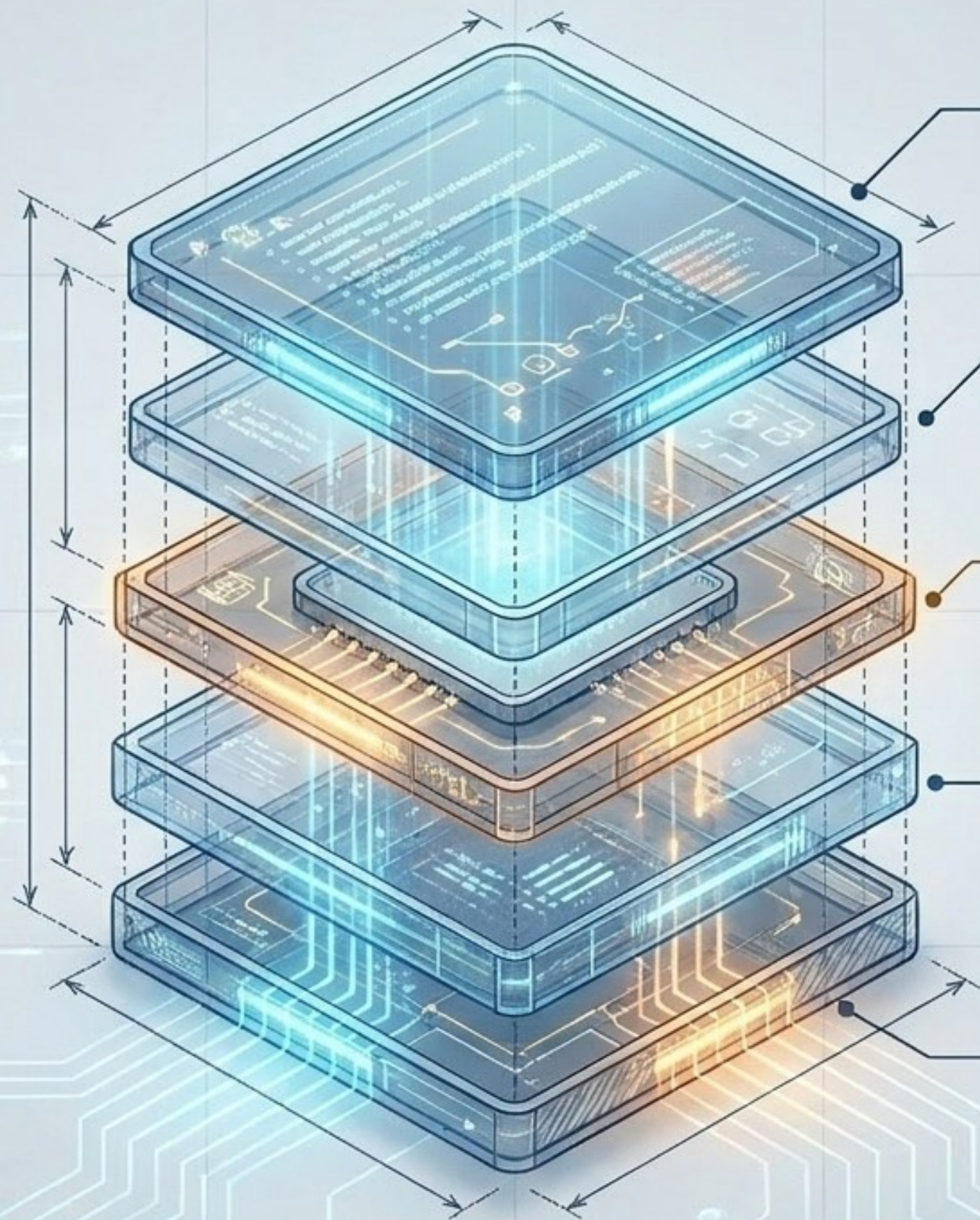
建立標準詞彙、模組與邊界

Level 1: 試錯法 (Trial & Error)

依賴直覺，無法規模化



指令模塊解剖圖



1. 角色賦予 (Role)
定義模型領域知識邊界

2. 脈絡注入 (Context)
提供精確的背景數據與狀態

3. 任務清晰度 (Task)
無歧義的具體指令

4. 輸出結構 (Format)
定義資料型態
(如 JSON, Markdown)

5. 護欄與限制 (Guardrails)
設定禁制事項與安全邊界

主流框架比較矩陣：沒有銀彈，只有適配

	複雜度	重點優勢	最佳適用場景
COSTAR	高	語氣與格式的極致控制	商業溝通、行銷文案
CRISPE	中	探索性實驗	分析洞察、A/B 測試
BAB	低	情緒轉折與說服	客服挽回、銷售信件
ToT	極高	多步邏輯推理	技術除錯、複雜決策
RACE	低	極簡敏捷	高通量、快速部署的 內部工具

COSTAR 藍圖：GPT-4 提示大賽冠軍架構



致勝關鍵：將『格式呈現 (Style)』與『情感語氣 (Tone)』徹底分離，賦予 AI 雙維度的精準控制力。

資源受限環境的困境： 地端小模型的極限

COSTAR
複雜提示模塊
(巨量 Context)



認知過載
(Cognitive Overload)
& Token 耗盡

地端小模型
(Local LLM)



提示工程無法完全彌補模型能力的先天限制，在資源受限環境下，複雜框架常導致系統當機或回傳空泛內容。

COSTAR-A：為小模型注入強制決斷力



Answer (強制解答)

單一選擇決斷率

0% → 100% ✓

Yi-Coder-1.5B 模型實測數據

決斷性輸出 (Decisive Output)

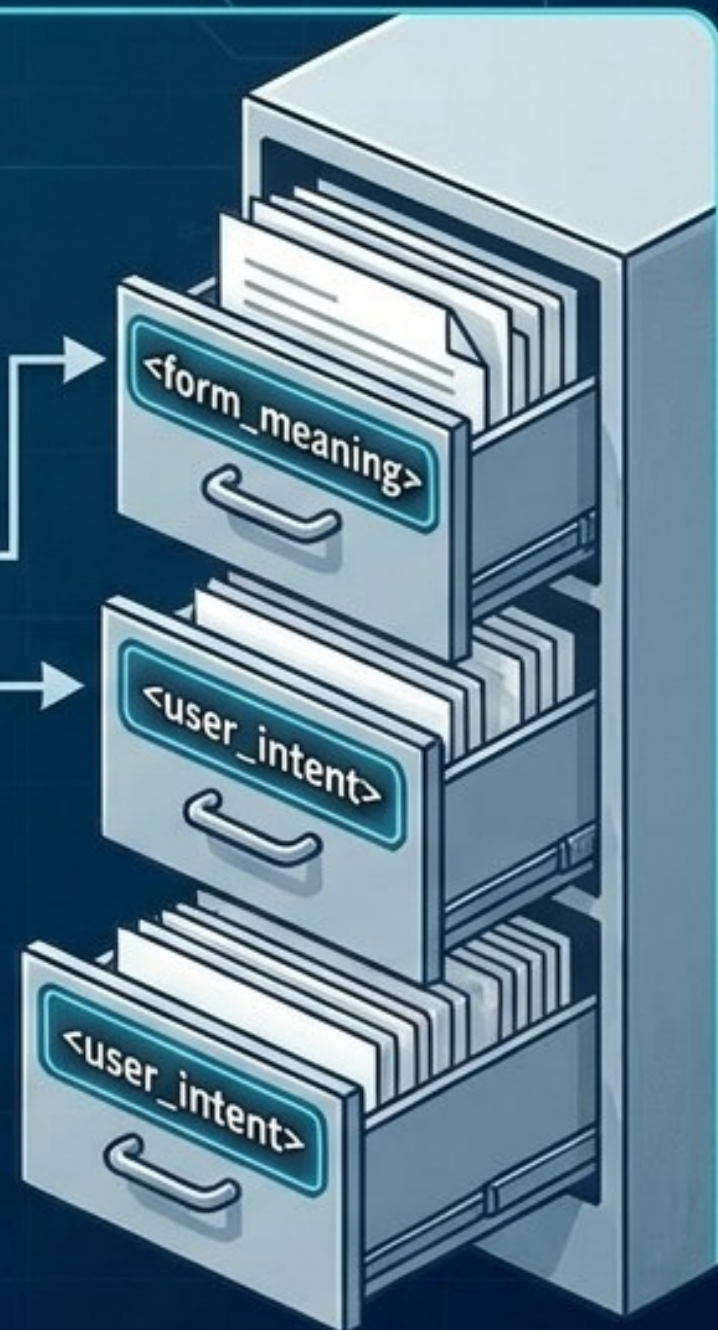
Anthropic 高階架構：XML 標籤與預填回應

✗ 散文式提示 (易混淆)



✓ XML 標籤封裝 (精確讀取)

```
<background_data>
... data ...
</background_data>
<instructions>
... tasks ...
</instructions>
```



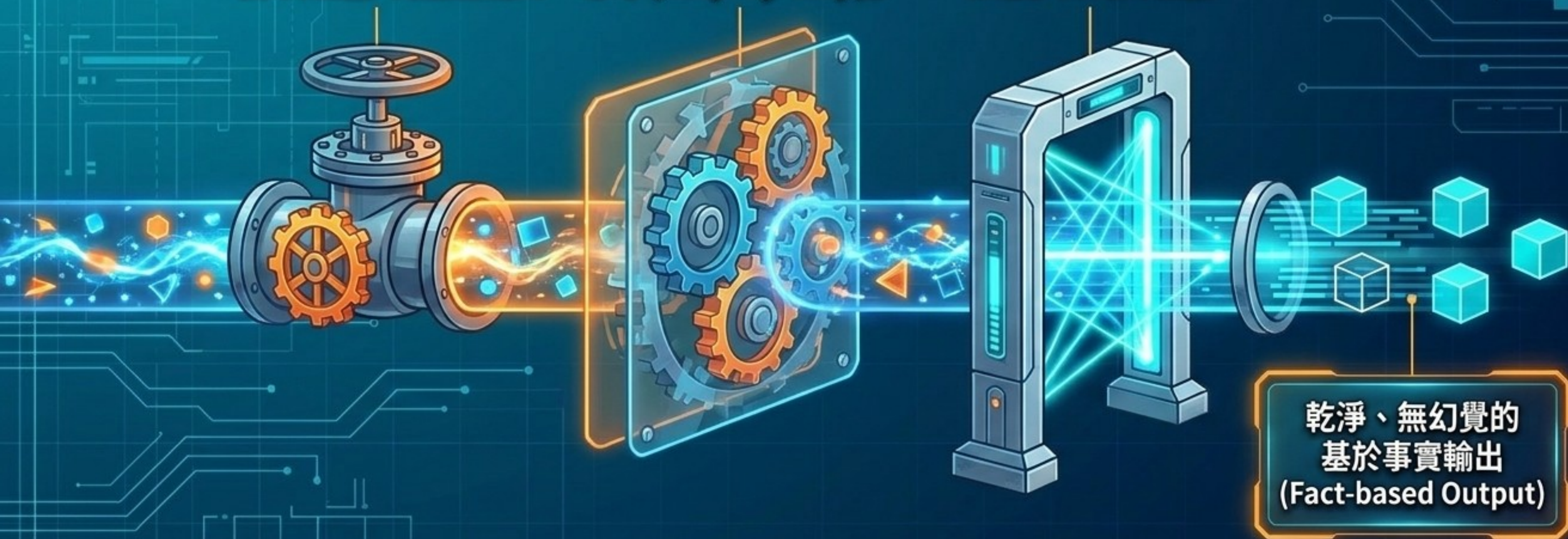
預填回應 (Prefilled Response)：在提示結尾輸入 { 或 <final_verdict>，強制模型繞過廢話，直接輸出 JSON 或目標格式。

阻斷幻覺：零信任的提示過濾機制

第一層：准許說
『我不知道』的逃生出口

第二層：強制『一步步
思考 (Step-by-step)』

第三層：強制『引用
來源』的對齊檢查



透過任務排序 (Task Ordering) 強制模型先檢查證據、再推理、最後才下結論。

典範轉移：從提示工程到脈絡工程



克服脈絡衰退 (Context Rot)



AI 代理的長程記憶管理策略

1. 壓縮 (Compaction)



長對話歷史

摘要

2. 結構化筆記 (Structured Note-taking)



釋放主記憶體

NOTES.md

3. 子代理架構 (Sub-agent Architectures)



主代理
(Lead Agent)

子探索者
(Sub-agents)

未來的基礎設施：程式化與自動化



從混亂語言到自治系統的藍圖

頂層 (自主系統)：
脈絡工程 (Context Eng)、工具調用
(Tools)、記憶管理 (Memory)

中層 (動態控制)：
小模型適配 (COSTAR-A)
與防幻覺護欄

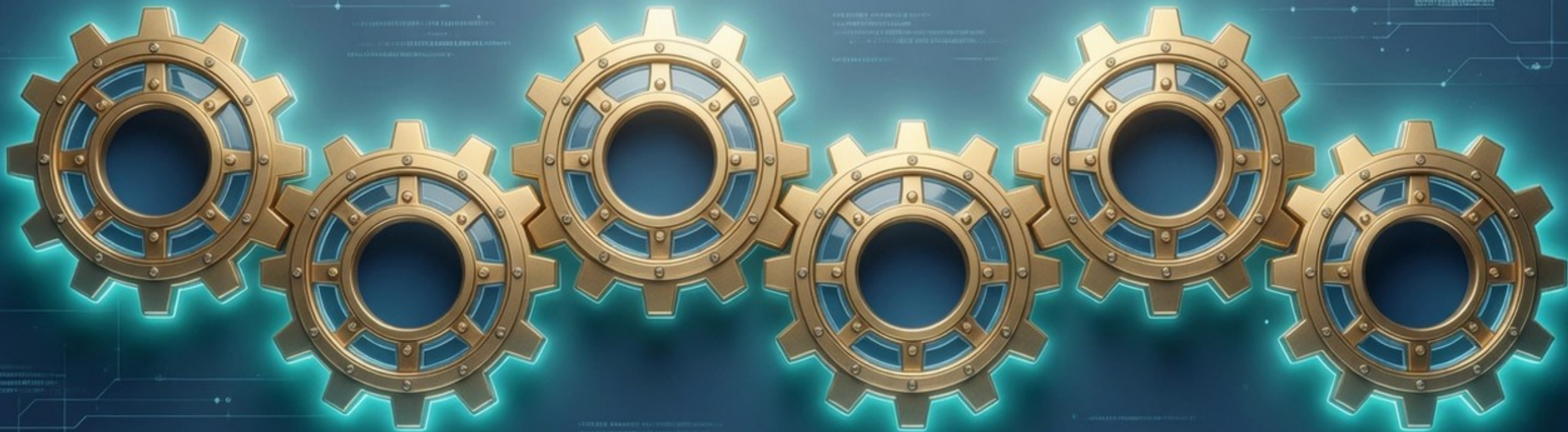
底層 (基礎設施)：
框架規範 (COSTAR / BAB / XML)



最好的提示工程，是將混亂的自然語言，轉化為具備工程可預測性的基礎設施。

附加 · 框架詳解 1/5 · C-O-S-T-A-R

COSTAR = Context · Objective · Style · Tone · Audience · Response



C Context

背景：而家發生咩事

O Objective

目標：想完成咩

S Style

格式：短訊／電郵

T Tone

語氣：軟／硬／堅定

A Audience

讀者：講俾邊個聽

R Response

規格：字數與禁止

致勝關鍵：Style（格式）同 Tone（語氣）分開寫。適合對外溝通、文案。

COSTAR = Context · Objective · Style · Tone · Audience · Response

請用 COSTAR (Context, Objective, Style, Tone, Audience, Response) 。繁體中文。

C Context (背景) : 我喺香港網店買咗書，話 8 月 18 日到，而家 21 日都未出貨。

O Objective (目標) : 24 小時內確認新到貨日；若再遲要補償。

S Style (格式) : WhatsApp 短訊，分段，唔好寫成長電郵。

T Tone (語氣) : 有禮但堅定，唔好發脾氣。

A Audience (讀者) : 網店客服 (唔認識我) 。

R Response (規格) : 80 字內；結尾俾 2 個可選日期；唔准發明訂單編號。

附加 · 框架詳解 2/5 · C-R-I-S-P-E

CRISPE = Capacity · Role · Insight · Statement · Personality · Experiment



C Capacity

能力：邊方面專家

R Role

角色：對住邊個

I Insight

洞察：已知／未懂

S Statement

任務：要產出咩

P Personality

個性：鼓勵、嚴謹

E Experiment

實驗：再試一版

少寫 E Experiment 就叫 CRISP。適合功課輔導、分析兩種答法。

CRISPE = Capacity · Role · Insight · Statement · Personality · Experiment

請用 CRISPE (Capacity, Role, Insight, Statement, Personality, Experiment) 。繁體中文。

C Capacity (能力) : 你是耐心的中學通識老師，擅長教長題結構。

R Role (角色) : 對象是正在溫習考試的中五學生。

I Insight (洞察) : 我已經識「三權分立」名詞，但唔識點用嚟答 8 分長題。

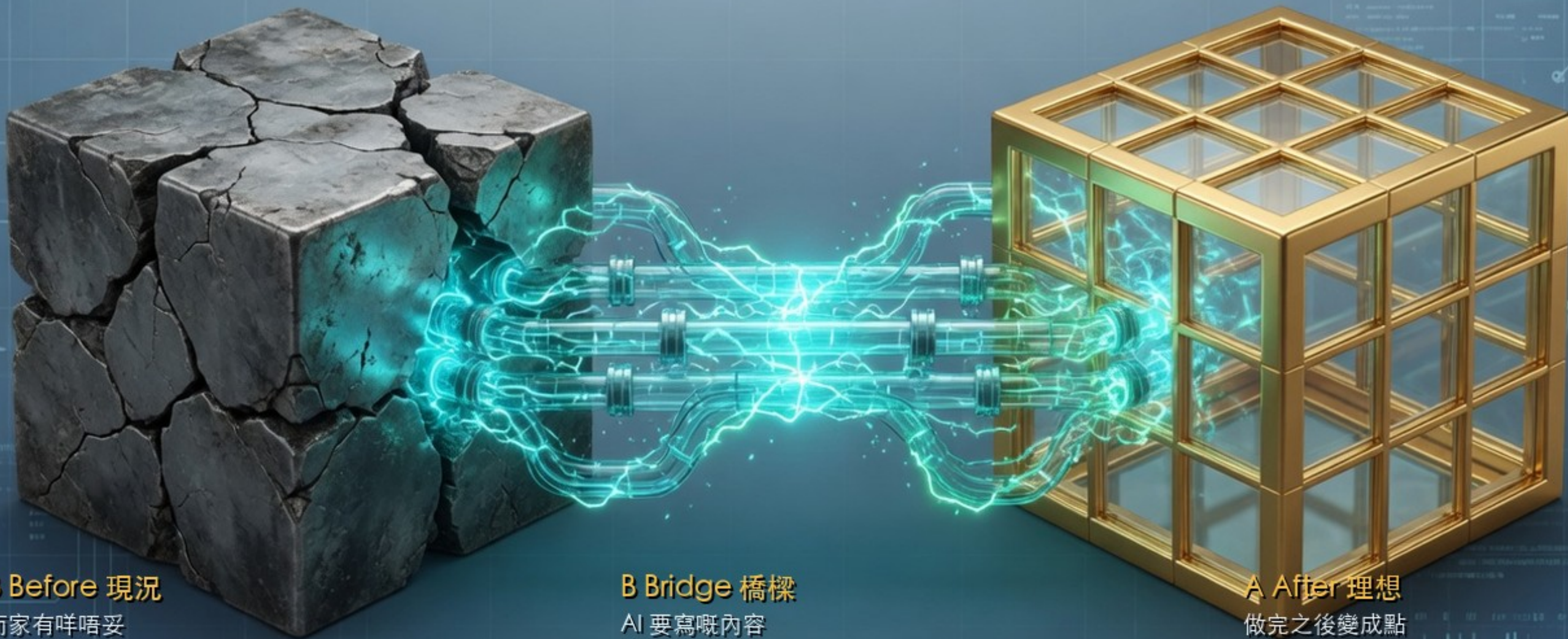
S Statement (任務) : 用一個香港例子，教我 8 分題應該分幾段、每段寫咩。

P Personality (個性) : 鼓勵、問我已知邊一步；唔好朗誦定義。

E Experiment (實驗) : 最後再給 1 條更難的對照題（只出題，唔好俾答案）。

限制：唔准直接寫可抄的完整答案。

BAB = Before · After · Bridge



B Before 現況

而家有咩唔妥

B Bridge 橋樑

AI 要寫嘅內容

A After 理想

做完之後變成點

一句講完：由痛到好，中間你寫橋。適合投訴、挽留、勸人。

BAB = Before · After · Bridge

請用 BAB (Before, After, Bridge) 。繁體中文。

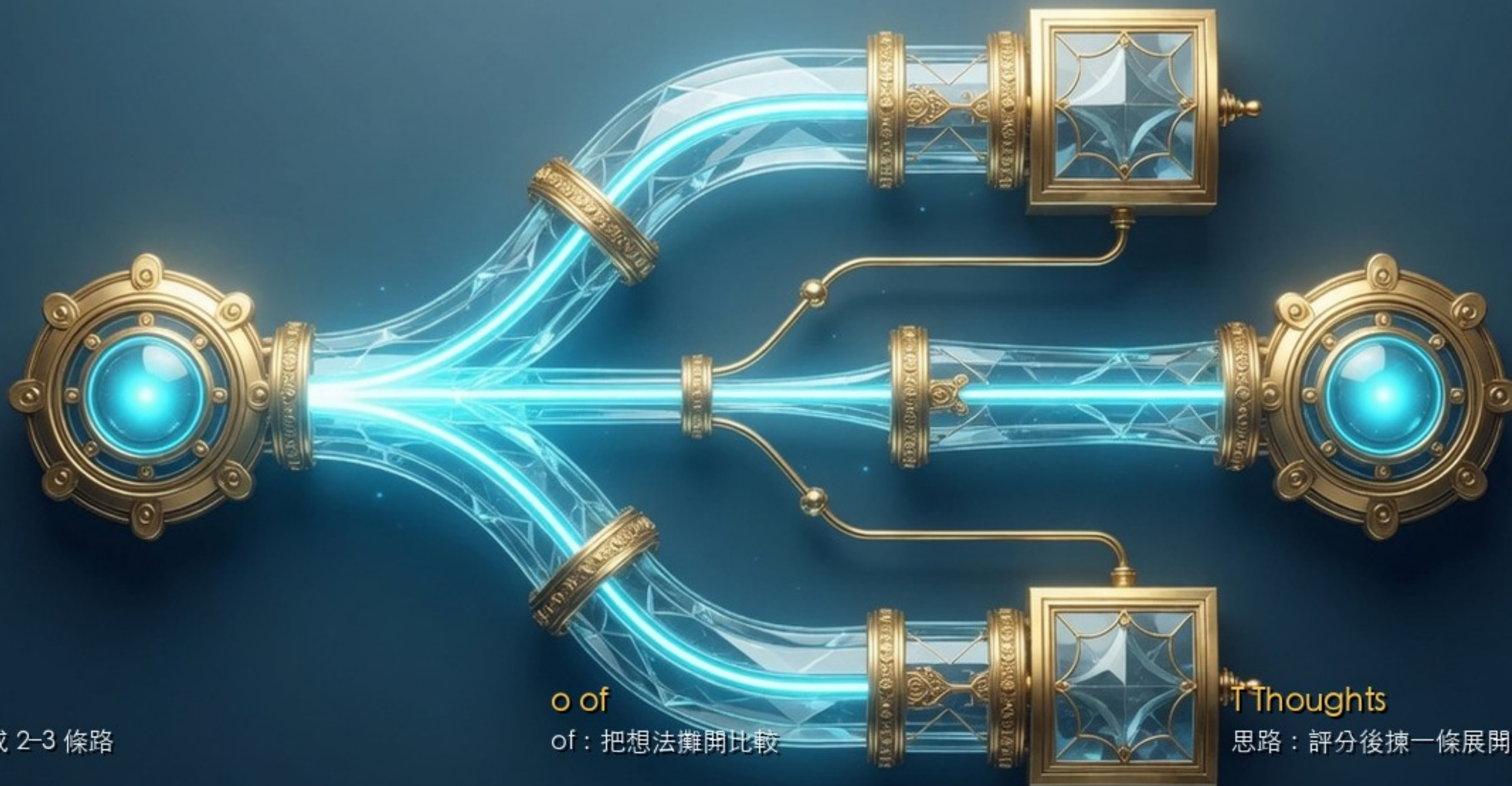
B Before (現況)：網店話 8 月 18 日到貨，而家 21 日都未出，我唔知幾時收到、無單號。

A After (理想)：24 小時內收到新到貨日；如果再遲，有補償方案。

B Bridge (橋樑／請你寫)：一封短電郵，把我由「焦慮」帶到「有下一步」。

限制：180 字內、有禮、分段、結尾問一個清楚問題。唔准發明訂單編號。

ToT = Tree of Thoughts (思維樹)



Tree of Thoughts：先列路 → 評分 → 揀最高分再寫細節。適合計劃、決策。

ToT = Tree of Thoughts (思維樹)

請用 ToT = Tree of Thoughts (思維樹／分岔思考)。繁體中文。

題目：我要 7 日內溫完光合作用。每日只有 30 分鐘。考試係 8 分短答。

第 1 步：先列出 3 個溫習策略（平均分日／先難後易／只背最常考）。

第 2 步：每個策略用「時間夠唔夠、記得唔記得、壓力大唔大」各評 1-5 分。

第 3 步：揀總分最高嗰條，寫成 7 日時間表（每日 30 分鐘做咩）。

限制：唔好一開始就只給一個答案。唔准發明我有講過的考試日期。

RACE = Role · Action · Context · Expectation

R Role 角色

你是誰

你是家庭理財助理

A Action 行動

要做咩

整理超市單 + 慳錢計劃

C Context 背景

已知條件

兩公婆、伙食 \$4000、想減 \$500

E Expectation 期望

輸出規格

5 點摘要 + 3 個可執行動作

四缺幾乎一一對應。初學者由 RACE 起功。

RACE = Role · Action · Context · Expectation

請用 RACE (Role, Action, Context, Expectation) 。繁體中文。

R Role (角色) : 你是家庭理財助理，語氣務實、唔嚇人。

A Action (行動) : 把我貼上的超市單整理成下月慳錢計劃。

C Context (背景) : 兩公婆、每月伙食約 \$4000、想減 \$500；單據：【貼上】

E Expectation (期望) : 1) 最多 5 點摘要 (標出最大開支) 2) 3 個下月可執行慳錢動作 3) 唔准發明單據上沒有的價格或日期

差：「幫我慳錢。」 好：角色 + 行動 + 背景 + 期望，四格寫完就可以貼。

HKMAC · Hong Kong Makers AI Community

掃碼進入 hkmac.ai



<https://hkmac.ai/>

工作坊 · 講義 · 實作提示 · 免費面對面實體堂