

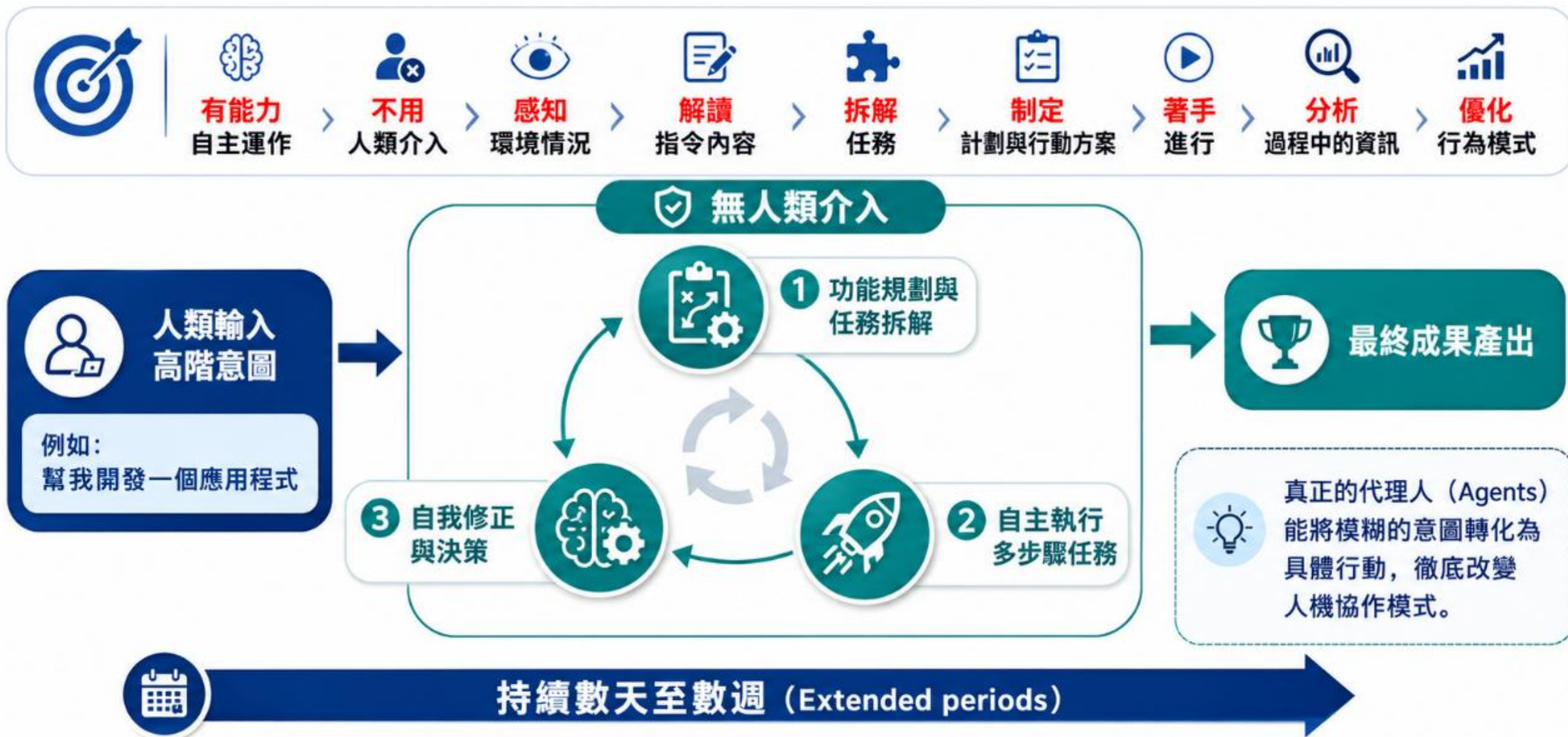
單元二： AI Agent與品質分析

AI代理的崛起：從輔助工具到數位員工

- AI正從**基於提示的內容生成**，躍升為目標驅動的自主執行，多智能體的協作將重塑企業核心生產力



AI Agent是什麼？

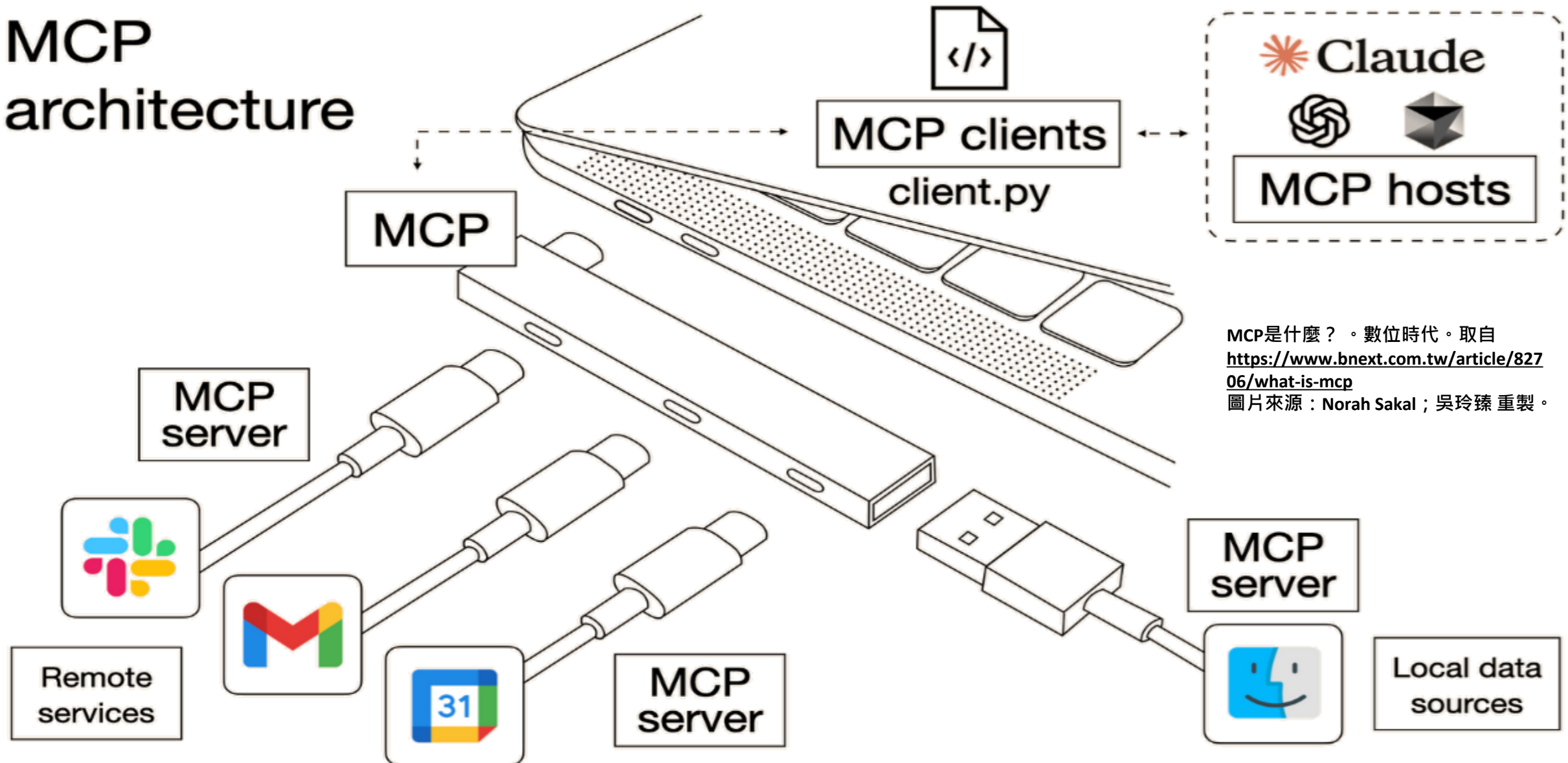


AI Agent應該具備哪些能力？



模型上下文協定 (Model Context Protocol, MCP)

MCP architecture



MCP是什麼？。數位時代。取自
<https://www.bnext.com.tw/article/82706/what-is-mcp>
圖片來源：Norah Sakal；吳玲臻 重製。

AI Agent 最新應用

- 近年最受矚目的二款 AI Agent，正在改變個人助理與軟體開發的工作方式



OpenAI Codex

雲端軟體工程代理人

- OpenAI 推出的 AI 程式設計代理人
- 可寫功能、改 Bug、執行測試、提交程式檢測



Claude Code

Anthropic 終端機代理

- Anthropic 推出的代理式編碼工具
- 能理解整個專案、跨檔案修改、執行測試
- Dispatch 可以遠端自動操控電腦

OpenAI Codex — 雲端軟體工程代理人

• 從Codex CLI到Codex桌面App擴充執行環境，一年內躍升為主流開發工具



開發者
OpenAI

首次發布
2025 年 4 月 (Codex CLI 命令列工具)

使用規模
2026 年 3 月週活躍用戶突破 200 萬

支援平台
macOS / Windows 桌面 App、VS Code、Cursor、JetBrains

1 多代理並行：Codex App 統一指揮中心

2026 年 2 月推出桌面 App，可同時管理多個代理執行緒、用 Worktree 隔離環境，跨專案、跨任務並行運作，把以往需數週的工作壓縮到數天完成。

2 長任務自動化：Skills、Automations 與記憶

Skills 將工具、腳本與指引打包，讓 Codex 處理研究、寫作等非寫程式工作；Automations 在背景定時執行 issue 分流、CI 監控；記憶功能保留個人偏好與專案脈絡。

3 原生電腦操作：GPT-5.4 加入 Computer Use

GPT-5.4 為首款具原生電腦操作能力的通用模型，能跨應用執行長期任務；亦推出 Chrome 擴充元件，可在背景平行操作多個瀏覽器分頁。

4 資安代理：Codex Security

應用程式安全代理，先建立程式庫威脅模型再尋找漏洞；30 天內檢測 120 萬筆 commit，於 Chromium、OpenSSL 等專案找出近 800 個高危漏洞。

Claude Code — Anthropic 的代理式編碼系統

- 從終端機指令到桌面App，能讀整個程式庫、跨檔案修改、執行測試並提交 PR



開發者

Anthropic

支援模型

Claude Opus 4.7、Sonnet 4.6、
Haiku 4.5

SWE-bench

Claude Mythos 達 93.9%，業界領先

使用方式

終端機 CLI、VS Code / Cursor /
Windsurf 擴充、JetBrains、桌面
App、瀏覽器

1 專案層級的代理：不只補全，是接管整段任務

可讀取整個程式庫、跨多檔案規劃變更、執行測試並依錯誤迭代修復；Anthropic 內部**大多數程式碼**現由 Claude Code 撰寫。

2 多代理協同：Claude Managed Agents

2026 年 5 月發表多代理協作 (Multi-Agent Orchestration)、目標導向 (Outcomes) 與 **Dreaming** 自我反思——可組成代理艦隊處理複雜任務並從歷次 Session 中自我改進。

3 Computer Use：跨越程式碼之外

能控制瀏覽器與 GUI 完成端到端測試、表單填寫、儀表板驗證等工作；單一代理迴圈即可整合外部系統，毋須切換到其他自動化工具。

4 Skills 與 Plugin 生態

Skills 機制讓使用者打包指引、腳本與資源以擴充能力；社群已建立大量 Skills 市集，並支援 MCP 連接 GitHub、GitLab、Linear、Slack 等開發協作工具。

AI時代新貨幣？

黃仁勳喊

「發Token當薪水」

科技業薪酬第4要素



「發Token當薪水」

黃仁勳

NVIDIA 創辦人暨執行長

AI 領航者 · 運算未來

1

傳統薪酬結構



- 固定薪資
- 獎金
- 股票 / 股權

2

第4要素：Token



- 數位資產型激勵
- 可與企業生態系連動
- 可能具流通與增值潛力

4

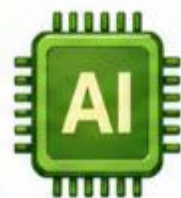
企業可能優勢



- 激勵創新
- 提高留才效果
- 連結長期績效

3

為何在AI時代被重視



- 吸引A 與科技人才
- 強化員工與公司共同成長
- 建立社群與平台參與感

科技業 薪酬第4要素

傳統三要素 + Token
開啟薪酬新時代

5

潛在風險與挑戰



- 價格波動
- 法規與稅務問題
- 員工接受績差異
- 制度設計複雜

6

未來意涵



- 薪酬從現金走向資產化
- 人才競爭模式改變
- 科技業可能率先試行



人才為本



Token 激勵



共同成長



創造長期價值

AI 在電子製造業的典型應用情境

1 品質檢測

- ✓ AOI 焊點與 PCB 瑕疵辨識
- ✓ 錫膏印刷異常判讀
- ✓ 良率預測



2 設備管理

- ✓ 貼片機預測性維修
- ✓ 稼動率與換線損失分析
- ✓ 異常代碼處理建議



SMT、組裝、測試

可用於各個生產環節，
提供不同價值

3 排程與接單

- ✓ 多機種少量換線排程模擬
- ✓ 客戶 BOM 與規格審核
- ✓ 工程圖與單據辨識



4 跨部門溝通

- ✓ 製程與良率報告自動生成
- ✓ 異常原因說明
- ✓ 工程知識管理



導入 AI 的關鍵不在於技術，而在於**是否解決真正的營運痛點。**

品質檢測 – 電子製造產業

01 應用重點



AI 在電子製造領域
應用多元且深入



尤其在 **SMT 製程**
與 **品質檢測** 成效顯著



AI 品質檢測 應用

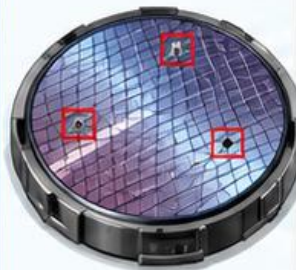
02 PCB 焊點品質檢測

AOI攝影機



- ✓ 電子代工廠導入 AI 視覺檢測系統
把關 **PCB 焊點品質**
- ✓ 以高解析影像搭配深度學習模型比對焊點外觀
- ✓ 辨識：假焊、少錫、元件偏移等細微瑕疵
- ✓ 過濾 AOI 的假不良，降低人工複判工時

03 晶圓缺陷分析



- ✓ 半導體廠以 AI 進行**晶圓缺陷**分類與影像比對
- ✓ 自動**辨識缺陷**樣態
- ✓ 回溯**關聯機台**與**製程參數**
- ✓ 加快異常原因鎖定與**良率改善**速度

04 延伸效益



設備預防保養

預測設備異常
降低故障停機風險



製程參數優化

AI 分析關鍵參數
優化製程條件



強化生產穩定性 與**成本效益**

提升良率與穩定性
降低成本、提升競爭力



AI 不只提升**檢測準確度**，也加速**良率改善**與**營運優化**



排程與接單: A工業

- 企業概況

- A工業為**典型製造型中小企業**，資本額6,000萬新台幣，員工數不到200人，主要從事各類線材的研發與製造

- 客戶突襲式要求

- 2024年6月24日，A工業在毫無預警下，接獲歐洲大廠在台分公司發出的**碳減排計畫**信函，並在一週內先後4次催促完成碳盤查認證與官網英文化。

- 減排指標嚴苛

- 9月26日，該客戶再度明確要求：2030年前，範疇一與範疇二溫室氣體排放須減少50%、範疇三須減少15%，**並警告不符合將面臨取消訂單風險。**

A工業：導入AIoT實現減碳目標



2021年底**導入AIoT技術**
搭建**數位碳盤查**與**綠色供應鏈平台**
實現**節能減排**與**碳排查合規**目標



01 關鍵設備智慧化監測



關鍵生產設備加裝智慧電錶



AIoT定量監測耗能



每月自動產出分析報表



取代人工抄錶流程



提升能源透明度與效率

02 零碳雲平台與碳盤查



零碳雲平台整合
合規管理工具



完成自有廠區
溫室氣體盤查



完成供應鏈
溫室氣體盤查

03 MES與RPA優化營運



導入MES與RPA技術



優化製造執行流程



強化供應鏈協同



減少能源浪費



提高生產效能



減碳



節能



合規



效率提升

AI 於生產流程之導入架構

- **第一階段 單機智慧化**

- 單一機台或工站導入 AI 模型，如：影像瑕疵檢測、單機振動異常偵測。
- 目標：點狀驗證 AI 可行性、累積資料與經驗。

- **第二階段 產線連網與資料整合**

- 透過 IoT 將多機台、MES、ERP 資料串接至雲端或邊緣伺服器。
- 建立統一的資料平台，支援後續預測模型訓練。

- **第三階段 跨部門 AI 應用**

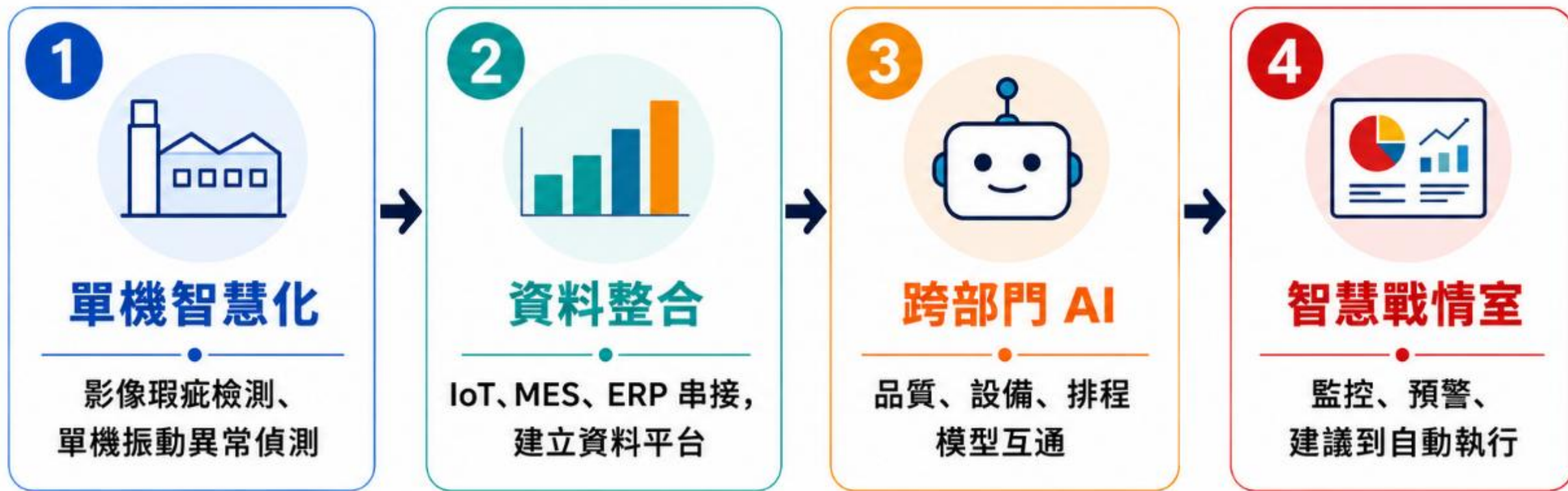
- 品質、設備、排程系統互通，AI 模型可橫跨多個業務環節。
- 引入生成式 AI 進行報告生成與決策說明。

- **第四階段 智慧戰情室 (AI Agent 閉環)**

- AI Agent 整合各系統訊號、即時呈現營運儀表板。
- 從監控、預警、行動建議到自動執行，形成決策閉環。

AI 於生產流程之導入架構：四階段路徑圖

- 從單機驗證開始，逐步把資料、模型與決策流程串成營運循環。



關鍵轉折：不是一次導入所有 AI，而是讓每一階段都累積
下一階段需要的資料與管理經驗。

資料保護與隱私

- 資料保護與隱私：開發者需確保AI系統遵循相關法律法規，保護用戶的隱私與資料安全，防止資料濫用。
- 企業在導入AI時，需尊重顧客個人資料並確保資料安全。
 - 企業的CRM與AI系統通常仰賴大量顧客資料，如消費記錄，因此企業必須取得合法授權並對敏感資訊進行匿名化、加密處理，以防止濫用或外洩。
 - 此外，企業在開發AI程式時應遵循相關隱私法規(GDPR, General Data Protection Regulation)來制定嚴謹的資料治理政策。
 - 資料安全同等重要，需建立強健的安全措施來防範資料遭未授權存取或 AI 模型遭惡意攻擊。
- 透過保障隱私與資料安全，企業才能在數位轉型中維持顧客信任。

使用AI工具的資安與營業機密守則

- **資料機密性**

- 訂單資料、製程參數、客戶資料...等都是公司營業機密與客戶個資。
- 資料一旦外洩，可能違反保密合約、個資法，甚至流入模型訓練無法收回。

- **上傳前先做去識別化**

- 移除或代換客戶名稱、料號、人名等可識別資訊，用代號取代(如: 客戶A)。
- 只上傳分析所需的最小資料量，不要整份 BOM、報價或合約全貼上去。

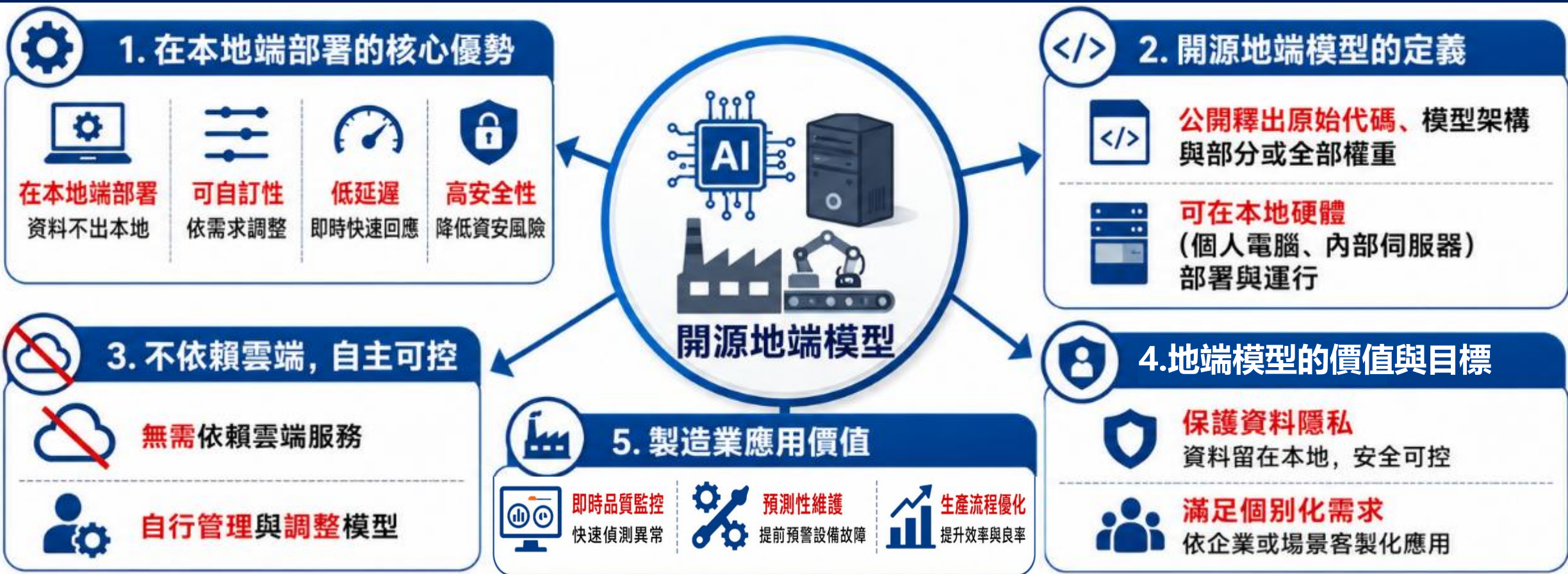
- **選對工具與設定**

- 使用企業版 / 團隊版，確認服務商不以你的資料訓練模型。
- 高度機密資料優先考慮**地端 / 私有部署**方案，避免上傳公有雲。

- **建立公司使用規範**

- 明訂哪些資料可上傳、哪些絕對禁止；指定可使用的工具與帳號。
- 導入前與資安、法務確認，並對全體員工教育訓練。

開源地端模型



主要特性與優勢



靈活度高
可按需求調整、
修改與優化模型



隱私保護
資料在本地運算，
降低外洩風險



即時響應
減少網路傳輸延遲，
提高系統反應速度

開源模型的硬體需求與現實限制

1 硬體需求：看模型大小決定



1 小型 3-8B (30 ~ 80 億參數)

筆電或單張顯卡可跑，
適合摘要、分類。



中型 30-70B (300 ~ 700 億參數)

需工作站級顯卡，
顯存約 40GB。



3 旗艦級 (數千億至兆級)

需多張伺服器顯卡，
建置與電費成本高。

2 使用上的主要缺點



能力通常落後
最新商用模型
半年到一年。



部署、更新、監控與
資安都要自己負責，
需要 IT 人力與
大量訓練費用。



授權條款不一，
「開源」不等於
可無限制商用。

黃仁勳於 COMPUTEX 宣示：地端 AI 時代來臨

NVIDIA 以企業級工具、開放模型與 Windows AI PC 架構，推動 AI Agent 從雲端走向地端



1 一、事件重點



在 COMPUTEX 相關發表中，黃仁勳強調 AI 正從雲端走向地端與個人裝置。



核心方向：讓 AI Agent 能在企業內部系統、邊緣設備與 AI PC 上執行。



代表意義：更低延遲、更好隱私、更高可控性

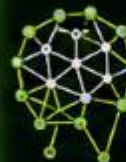
2 二、NVIDIA 兩大關鍵發布

NVIDIA Agent Intelligence Toolkit



- 開源工具套件
- 用於建立、串接、評估、監控與優化 AI Agent 工作流程
- 可鄭和多種代理、工具、記憶與檢索機制

NVIDIA Nemotron 開放模型



- 面相推理、程式、視覺與企業應用
- 支援開放下載、客製化與商業部署
- Nemotron 3 Ultra 主打長任務代理推理與更高效率

3 三、微軟合作重點



Microsoft 與 NVIDIA 推出面向 AI Agent 的新一代 Windows AI PC



以 NVIDIA RTX Spark + Windows 平台為核心



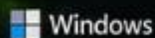
目標是讓代理型 AI 在本機端更有效率地運作



適合開發者、創作者與進階使用者



NVIDIA RTX Spark



4 四、對企業與產業的影響



企業：敏感資料可更傾向在地處理，提升治理與安全



開發者：更容易打造多代理應用、在地測試與部署



使用者：AI PC 逐步成為個人 AI 工作站



市場：AI 從「雲端服務」走向「端雲協同」



一句話總結：AI 不再只在雲端，而是開始真正進入企業地端與個人電腦。

Vibe Coding讓人人都能寫程式



電子製造業品質管理的常見挑戰



1 檢驗成本高、效率低

- 人工目視檢驗易疲勞，且新人培訓周期長。
- 抽樣檢驗無法全檢，仍可能讓不良品流出。



2 品質要因分析仰賴經驗

- 多變量交互作用，傳統 SPC 與魚骨圖難以涵蓋。
- 老師傅經驗無法系統化傳承。



3 良率預測落後

- 多數工廠仍以「事後檢驗」為主，無法提前介入。
- 缺乏跨製程資料整合，無法建立有效預測模型。



4 品質報告與知識管理零散

- 各廠區、各班別格式不一，比較困難。

品質檢測：AI 瑕疵檢測

- 在電子製造業，過去產品外觀與品質檢查多仰賴人工肉眼，費時費力且易有遺漏。
- AI 視覺瑕疵檢測利用高速相機與影像辨識模型，可大幅提升檢驗效率與一致性。
- 技術上多採用**卷積神經網路 (Convolutional neural network; CNN)**分析產品影像，模型經大量有瑕疵與無瑕疵樣本訓練，可**自動識別刮傷、斷裂等微小缺陷**。
- 如金屬扳手產品的外觀近照。透過高解析度相機取得產品影像，結合AI模型可檢測出表面**細微瑕疵**，降低人為檢測遺漏率。



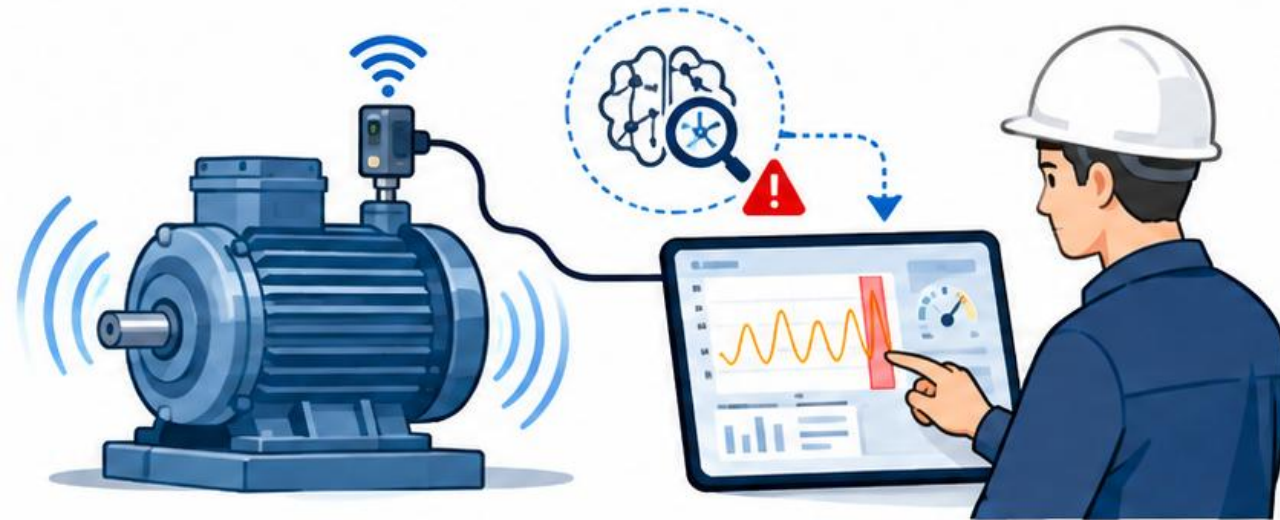
品質檢測：AI 異常識別

- 除外觀瑕疵，製程中的異常狀態也可由 AI 提早識別，共包含兩層面：
 - 其一是製程資料異常，例如**產品尺寸、溫度曲線**偏離正常範圍，可能意味品質問題。
 - 其二是設備狀態異常，如**機台震動或電流異常升高**，預示潛在故障。
- AI 模型可學習正常運行時感測器資料的模式，一旦監測到偏離正常範圍的資料點或模式突變，即視為異常並發出警示。
- 特別是在**預測性維護**方面，**預測式 AI** 扮演關鍵角色：透過對設備歷史運轉資料訓練的模型，可在故障發生前偵測出早期異常訊號(例如軸承震動頻譜異常)，提示維護人員主動檢修。
- 此方式降低**非計畫停機風險**，縮短停機時間**並節省維修成本**。如某工廠引入 AI 設備監控後，預估將停機時間縮短40%，大幅提升生產連續性。

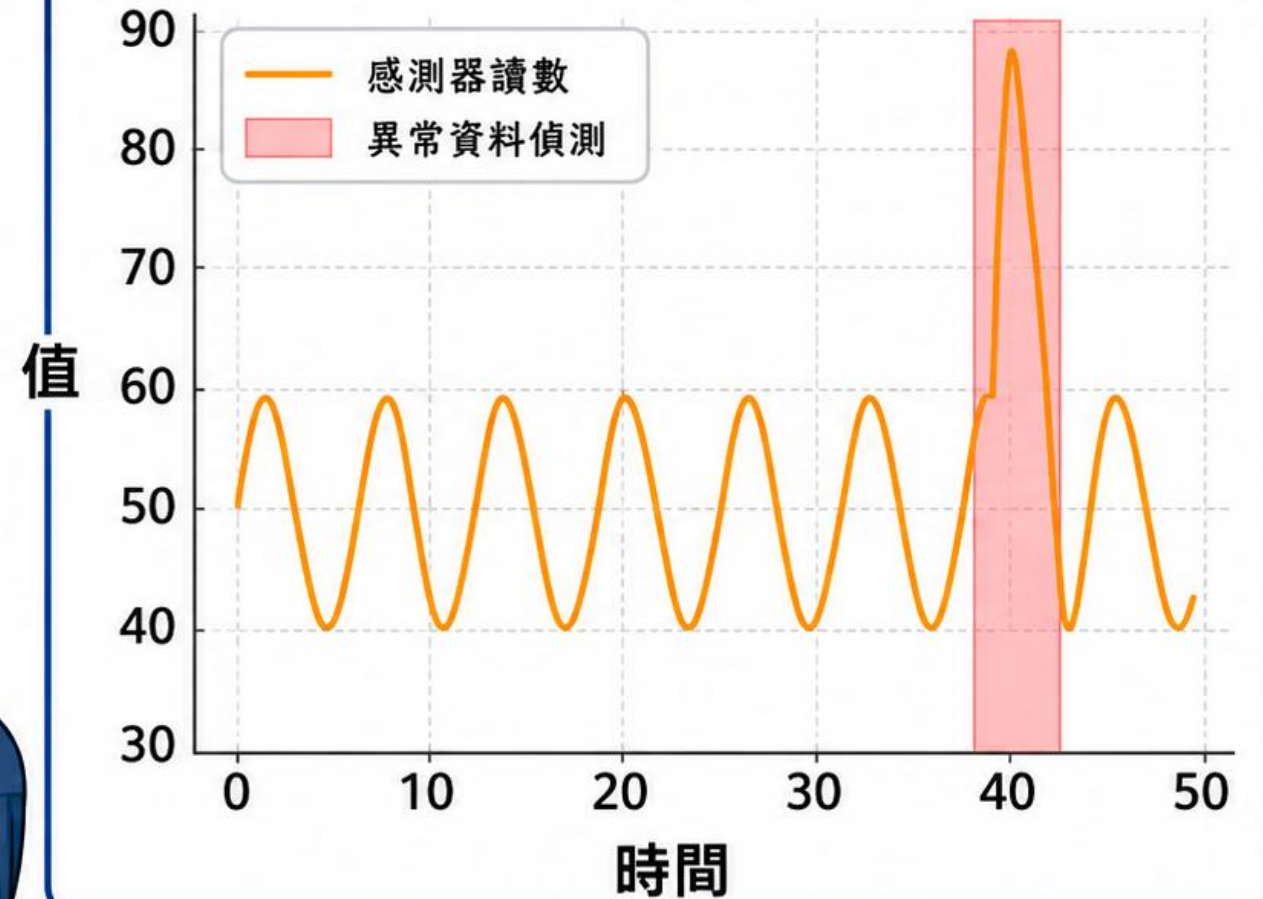
異常識別：設備振動

感測器資料中的異常偵測示意圖

橘色線表示設備振動數，
紅色區域為模型偵測出的異常範圍。
透過此類偵測，
可及早發現異常並採取措施。

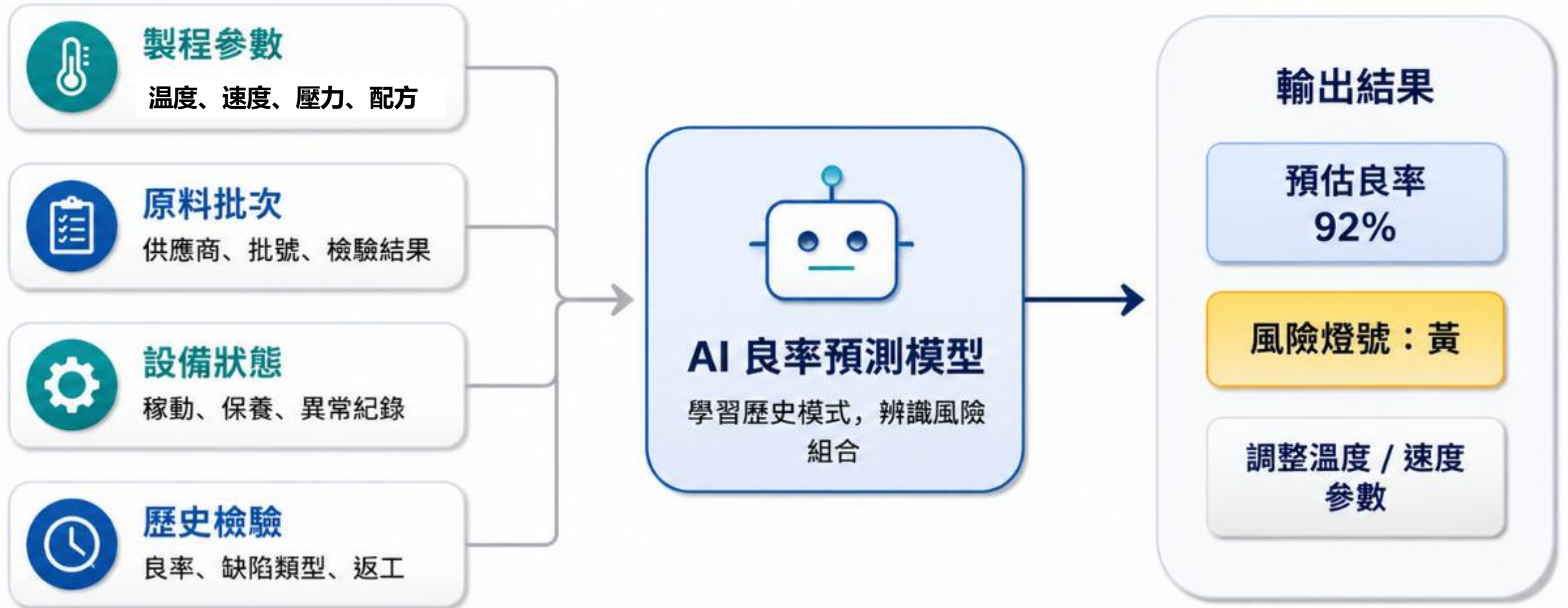


異常資料感測

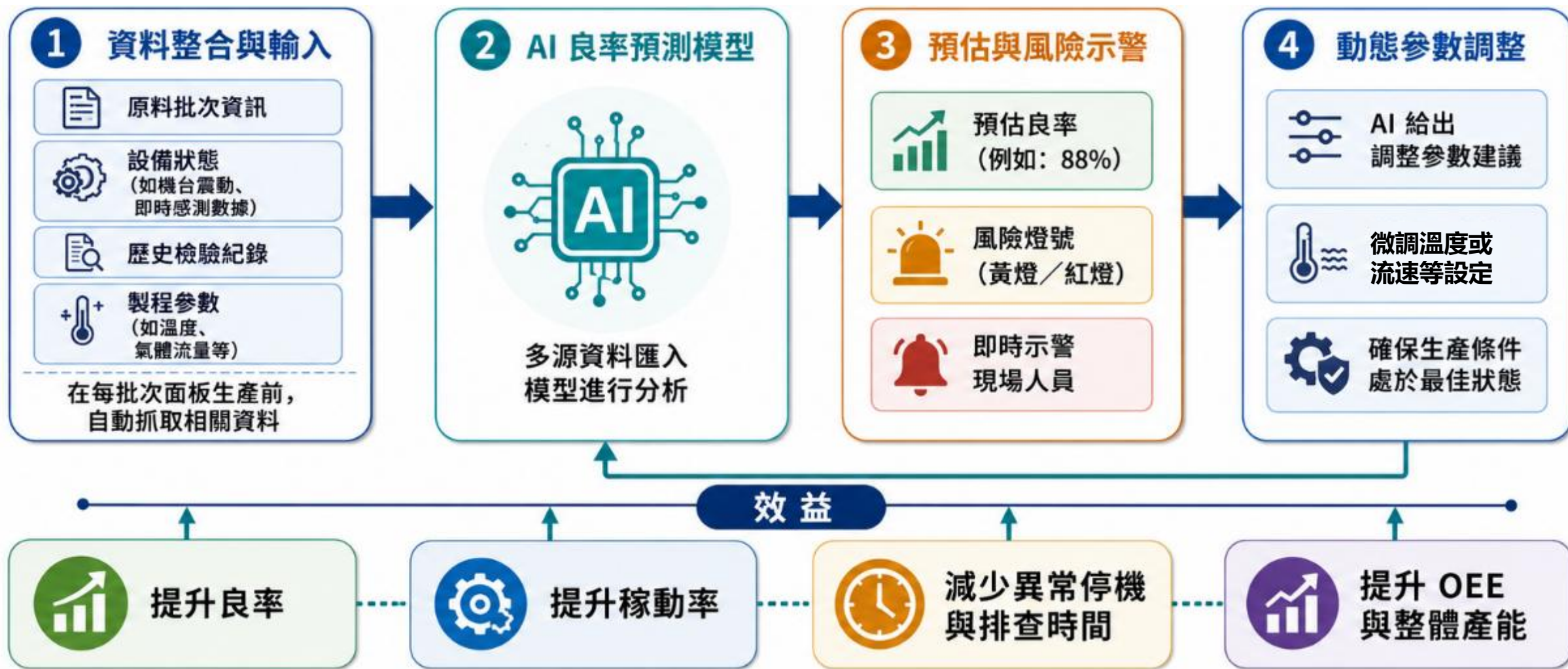


良率預測

- 把開機前可取得的資料匯入模型，先預估風險，再決定是否調整參數。



實務案例：AI 預測性生產與良率管理



透過 AI 精準補償與預測，提升產品整體良率，並有效強化設備稼動率與工廠產能。

AI 於品質決策支援



1 從單點檢測 走向決策支援



AI 不只判斷良/不良，更要能解釋**為什麼與該怎麼做**。



結合鑑別式 AI（找出問題）、預測式 AI（預估趨勢）、生成式 AI（產出建議）。



2 決策支援的 三層次

第一層
事實層



本批產品有多少良率？哪些缺陷類型最多？

第二層
原因層



哪些製程參數與不良率最相關？

第三層
行動層



建議如何調整參數、何時排修、如何撰寫報告？

應用數位孿生進行製造良率預測

- 不只模擬數位資訊，**包含工廠的物理環境（如：溫度、壓力...等）**，都一起進行模擬，獲得更準確的預測結果。



No-Code工具練習



No-Code 工具：ChatGPT 與 NotebookLM

- **ChatGPT**

- 通用型生成式 AI，可上傳圖片、表格進行解讀與分析。
- 適合：品質圖分析、要因推論、報告撰寫、SOP 草稿。

- **Google NotebookLM**

- 以**來源文件**為基礎的問答工具，可上傳多份品質報告、SOP 進行檢索。
- 適合：建立企業內部品質知識庫、新人查詢、跨報告比對。

- **No-Code 工具的優勢**

- 不需寫程式、不需資料科學家。
- 適合作為 AI 導入的試點驗證工具，快速驗證需求。

- **本單元將實際示範三個品質應用情境的 Prompt 設計。**



來源



+ 新增來源

試用 Deep Research 取得深度報告和新聞來源！

在網路上搜尋新來源



Fast Research
適合快速取得結果

Deep Research
深度報告和結果



已儲存的來源會顯示在這裡

點選上方的「新增來源」即可新增 PDF、網站、文字、影片或音訊檔案。你也可以直接從 Google 雲端硬碟匯入檔案。

對話



新增來源即可開始使用

上傳來源

上傳來源即可開始使用

0 個來源



工作室



語音摘要



影片摘要



心智圖



報告



學習卡



測驗



資訊圖表



簡報



工作室輸出內容會儲存在這裡。
加入來源後，點選即可新增語音摘要、研讀指南、心智圖等內容！

新增記事

實作1：品質要因分析

案例情境

某金屬加工廠生產「P-203 精密支架」，近期最終檢驗發現表面刮傷不良率明顯上升。

過去平均不良率約 2%–3%，但本週 B 班生產批次升至 11.8%。主管要求品保、製造與設備人員快速找出可能原因。

項目	內容
產品	P-203 精密支架
異常類型	表面刮傷
主要期間	6/3–6/5
主要班別	B 班
主要機台	M2
原料批號	AL-2406-B
原本平均不良率	2.5%
本週異常不良率	11.8%
近期變更	新進作業員 2 名、拋光輪更換供應商、M2 保養後重啟



實作1：品質異常批次紀錄

學員任務：請 AI 判斷哪些條件與不良率上升最有關。

批次	班別	機台	原料	操作員	拋光輪	保養狀態	不良率
B001	A	M1	AL-A	資深	W-01	正常	2.1%
B002	A	M2	AL-A	資深	W-01	正常	3.0%
B003	B	M2	AL-B	新手	W-02	保養後	10.8%
B004	B	M2	AL-B	新手	W-02	保養後	12.5%
B005	C	M1	AL-B	資深	W-02	正常	5.2%
B006	B	M3	AL-A	新手	W-01	正常	4.8%
B007	A	M2	AL-B	資深	W-02	保養後	7.6%
B008	C	M3	AL-A	資深	W-01	正常	2.4%
B009	B	M2	AL-C	新手	W-02	保養後	11.2%
B010	A	M1	AL-C	資深	W-01	正常	2.9%

實作1：Prompt 與預期輸出

可直接複製的 Prompt

以下是某製造廠的品質異常資料。請協助進行品質要因分析：

- (1) 依照人、機、料、法、環分類可能原因；
- (2) 使用 5 Why 分析最可能的根本原因；
- (3) 提出三個最優先驗證的假設；
- (4) 每個假設說明需要蒐集哪些現場資料；
- (5) 最後整理成品保會議可使用的表格。

預期輸出檢核

- 是否有依人、機、料、法、環分類，而非只列單一原因
- 是否把可能原因與待驗證假設分開
- 是否說明每個判斷依據來自哪筆資料
- 是否列出下一步需要補充的現場資料
- 是否能轉成會議討論表，而非只有文字敘述

實作2：品質良率預測

情境

生產線需在開機前預估今日批次的良率風險，並判斷是否需要調整製程參數。
請先用過去批次資料找出與良率最相關的線索，再針對新批次提出調整建議。

學員要回答

- 新批次屬於高、中、低風險？
- 最需要調整的 3 個參數是什麼？
- 哪些判斷仍需要正式模型或現場資料驗？

重要提醒：

生成式 AI 的預測屬於快速 PoC，非生產級模型。
後續仍需以正式機器學習工具驗證。

欄位	新批次設定
機台	M2
班別	B
原料	B
溫度	191°C
壓力	5.5 bar
速度	136 件/小時
濕度	69%
操作員經驗	新手

實作2：良率預測樣本資料

批次	機台	班別	原料	溫度	壓力	速度	濕度	經驗	良率
LOT-001	M1	A	A	180	4.8	120	55	資深	96.2
LOT-002	M1	A	A	182	4.9	118	56	資深	95.8
LOT-003	M2	B	B	190	5.4	135	68	新手	88.6
LOT-004	M2	B	B	192	5.6	138	70	新手	86.9
LOT-005	M3	C	A	181	4.7	121	57	熟手	94.9
LOT-006	M2	B	C	195	5.8	140	72	新手	84.7
LOT-007	M1	C	A	179	4.6	119	54	資深	96.8
LOT-008	M3	A	B	186	5.1	128	62	熟手	92.1
LOT-009	M2	B	B	193	5.5	136	69	新手	87.5
LOT-010	M1	A	C	184	5.0	124	59	資深	94.2
LOT-011	M3	B	B	188	5.3	132	66	熟手	90.3
LOT-012	M2	C	A	183	5.0	126	60	熟手	93.7
LOT-013	M1	B	A	181	4.9	122	58	新手	94.0
LOT-014	M2	B	C	196	5.9	141	73	新手	83.9

實作2：Prompt 與檢核重點

可直接複製的 Prompt

以下是過去批次產品製程參數與最終良率資料。
請協助分析：

- 哪些變數最可能影響良率？
- 高良率與低良率批次的主要差異為何？
- 針對新批次資料，請判斷良率風險高、中、低。
- 提出三項開機前可調整建議。
- 請提醒哪些結論只是初步判斷，仍需正式模型或現場驗證。

檢核重點

- AI 是否有指出變數關聯，而不是只描述單筆資料
- 是否把新批次歸為風險等級，而非假裝精準預測
- 是否給出開機前可執行的參數調整方向
- 是否提醒需用正式機器學習工具驗證