臺北商業大學
AI產業趨勢講座

Agentic AI 跨域研究與產業創新應用趨勢

Agentic AI Trends in Interdisciplinary Research and Innovative Industrial Applications

時間：2026/11/5 (四) 下午 12:00~13:30
地點：臺北商業大學 行政大樓7樓 第一會議室
主辦單位：國立臺北商業大學 研究發展處
(台北市中正區濟南路一段321號)



戴敏育 教授 (Prof. Min-Yuh Day)

國立臺北大學 資訊管理研究所 所長

跨域 AI 前瞻研究中心 (AI4X NTPU) 主任

2026-11-05



戴敏育 教授

Prof. Min-Yuh Day

NVIDIA University Ambassador
Certified Instructor

aws educate | Cloud Ambassador
2020 Cohort

aws academy Accredited Educator

aws certified Solutions Architect Associate

aws certified Cloud Practitioner

Director, Information Management, NTPU

Director, Intelligent Financial Innovation Technology, IFIT Lab, IM, NTPU

Director, Advanced Research Center for Cross-Disciplinary AI (AI4X), NTPU

CEO, Fintech and Green Finance Center (FGFC), NTPU

Visiting Scholar, IIS, Academia Sinica

Ph.D., Information Management, NTU

Artificial Intelligence, Agentic AI, ESG and Green Financial Technology, Big Data Analytics, Electronic Commerce

NTPU
國立臺北大學
National Taipei University

中央研究院 ACADEMIA SINICA 1928

國立臺灣大學

NTPU
國立臺北大學
National Taipei University
AACSB ACCREDITED

IM NTPU Information Management National Taipei University

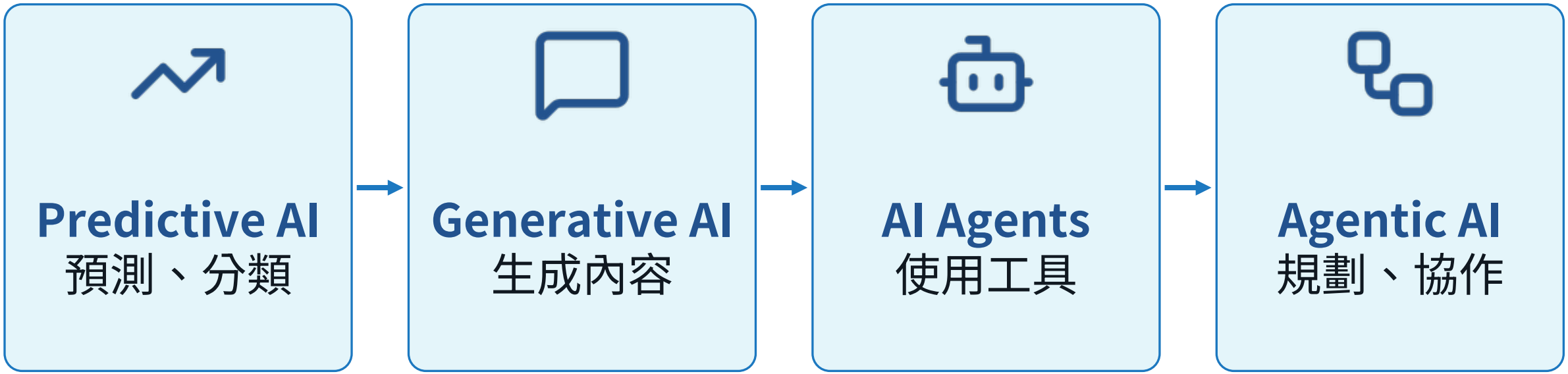
NTPU National Taipei University AI4X Research Center AI4X

Outline

1. AI 產業新典範：
   從回答問題到 Agentic AI 完成任務
2. Agentic AI 技術核心：
   Agent 架構與互通協定
3. 跨域研究前沿：
   研究問題與評測
4. 產業應用與國立臺北大學經驗：
   從情境到可驗證價值

From Generative AI to Agentic AI

技術演進與工作轉型



從內容生成，邁向自主執行
從單點智慧，邁向跨域協作；從技術展示，邁向產業價值

Agentic AI

Generative AI, Agentic AI, Physical AI

2012 AlexNet
Deep learning breakthrough

Perception AI
Speech recognition
Deep recommender systems
Medical imaging

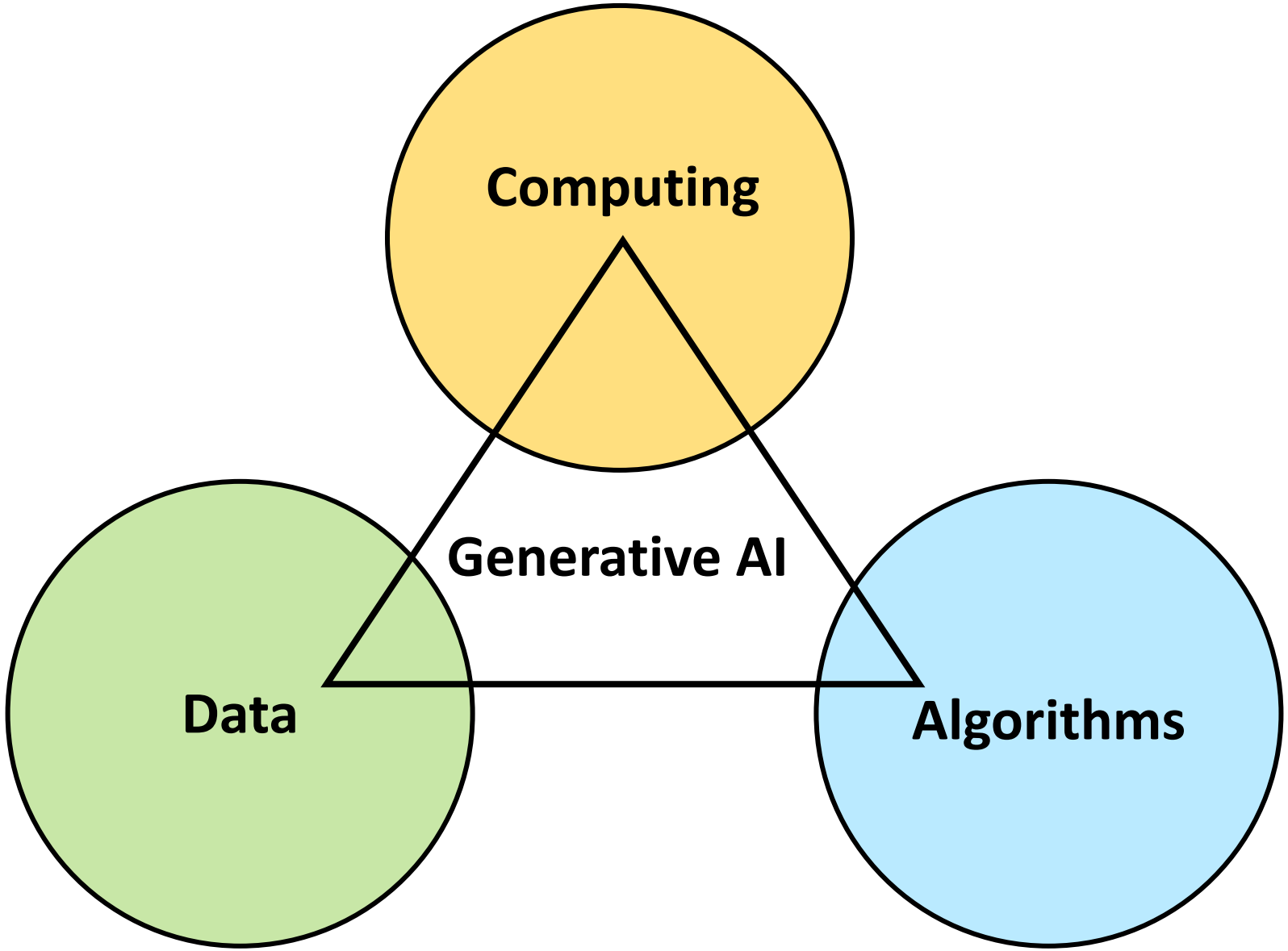
Generative AI
Digital marketing
Content creation

Agentic AI
Coding assistants
Customer service
Patient care

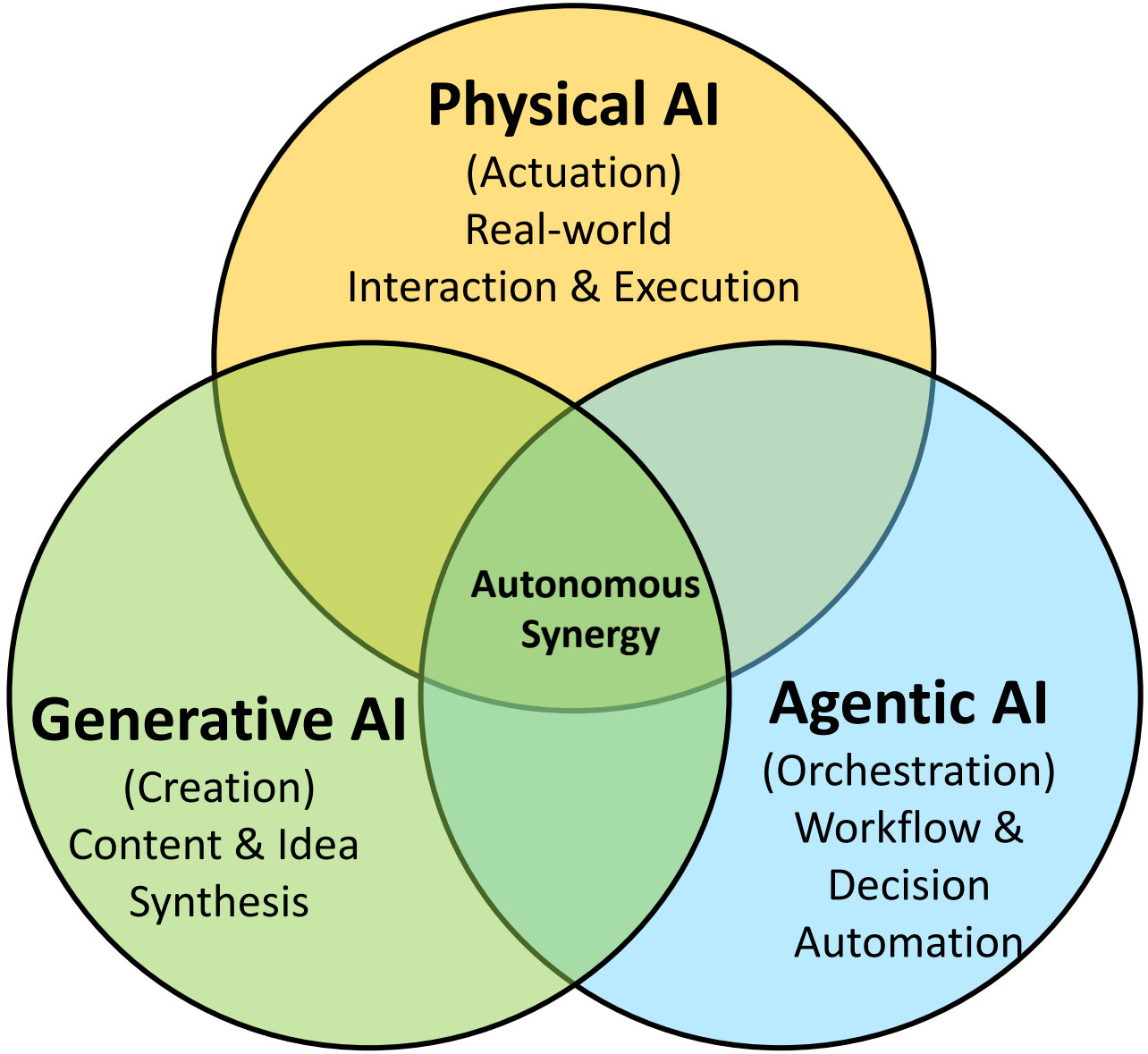
Physical AI
Self-driving cars
General robotics

Source: NVIDIA (2025), GTC March 2025 Keynote with NVIDIA CEO Jensen Huang, https://www.youtube.com/watch?v=_waPvOwL9Z8

Generative AI

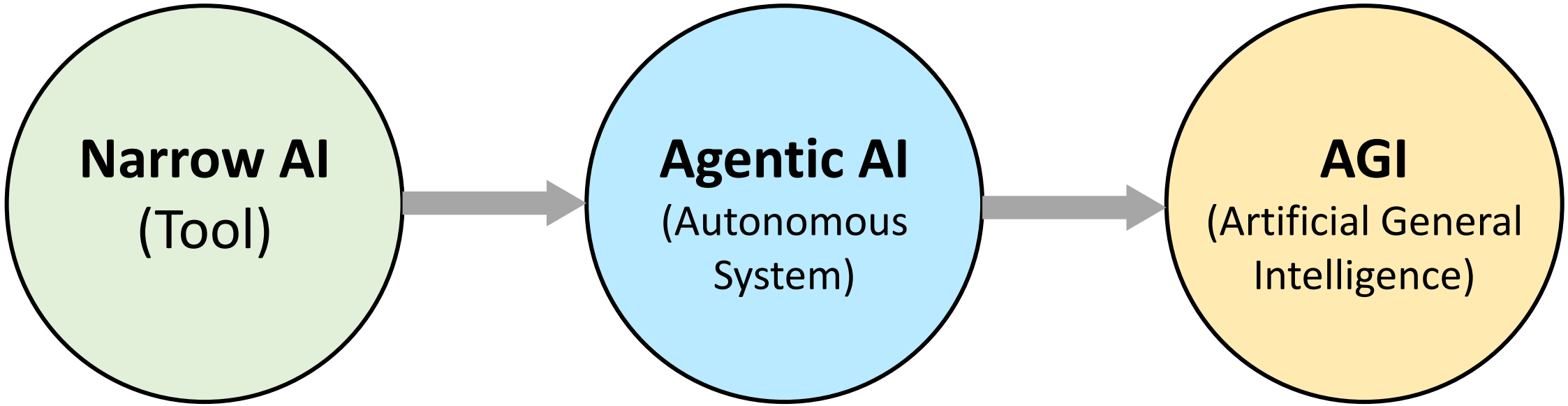


Generative AI, Agentic AI, Physical AI



New Economic Paradigm Shift: From Creation to Execution

The Future of AI
From Tools to Agents:
The Rise and Autonomy of Agentic AI

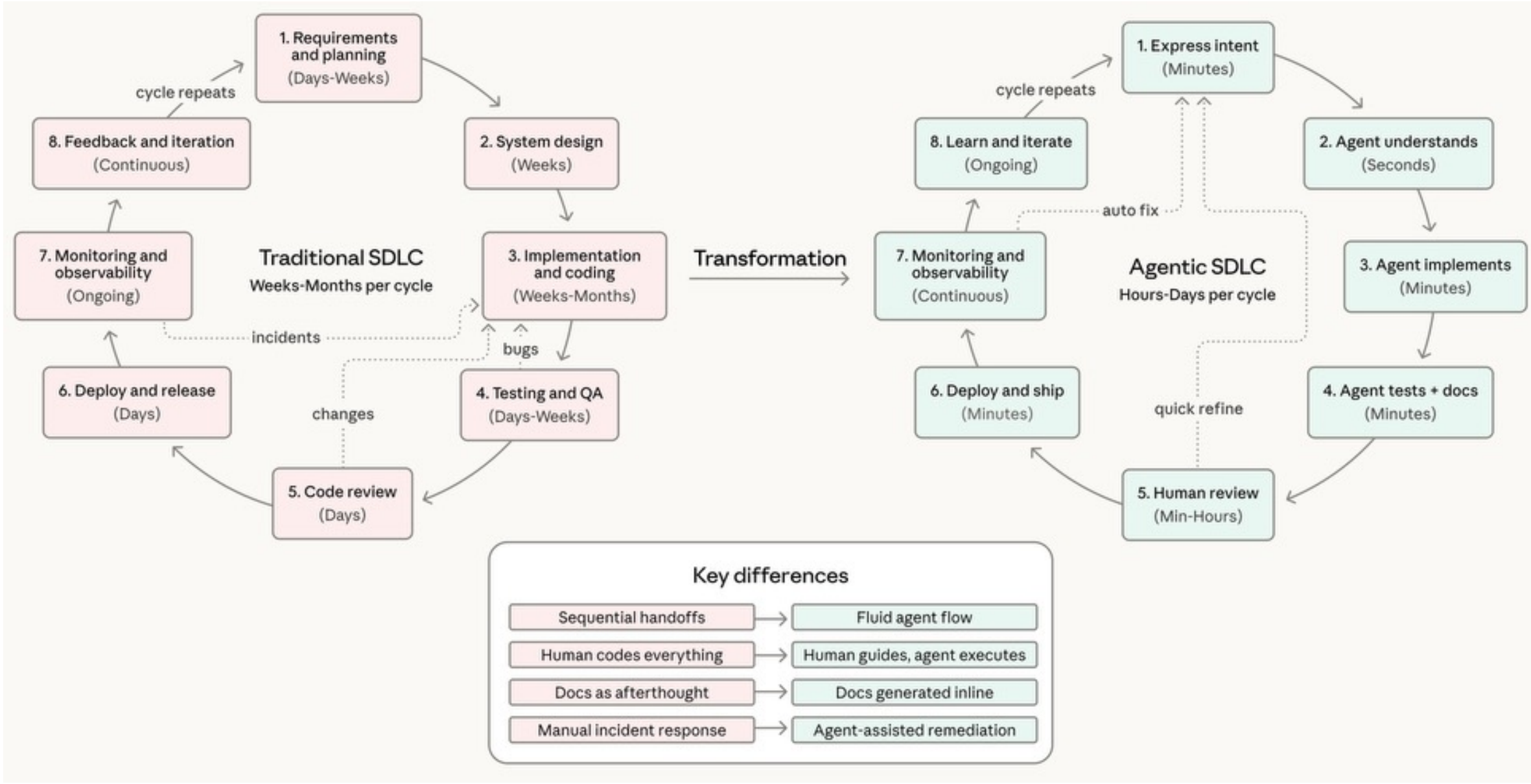


Executes Specific Tasks,
Content Generation

Goal-Oriented Behavior,
Autonomous Decision-Making,
Multi-Step Workflows,
Self-Improvement within Parameters

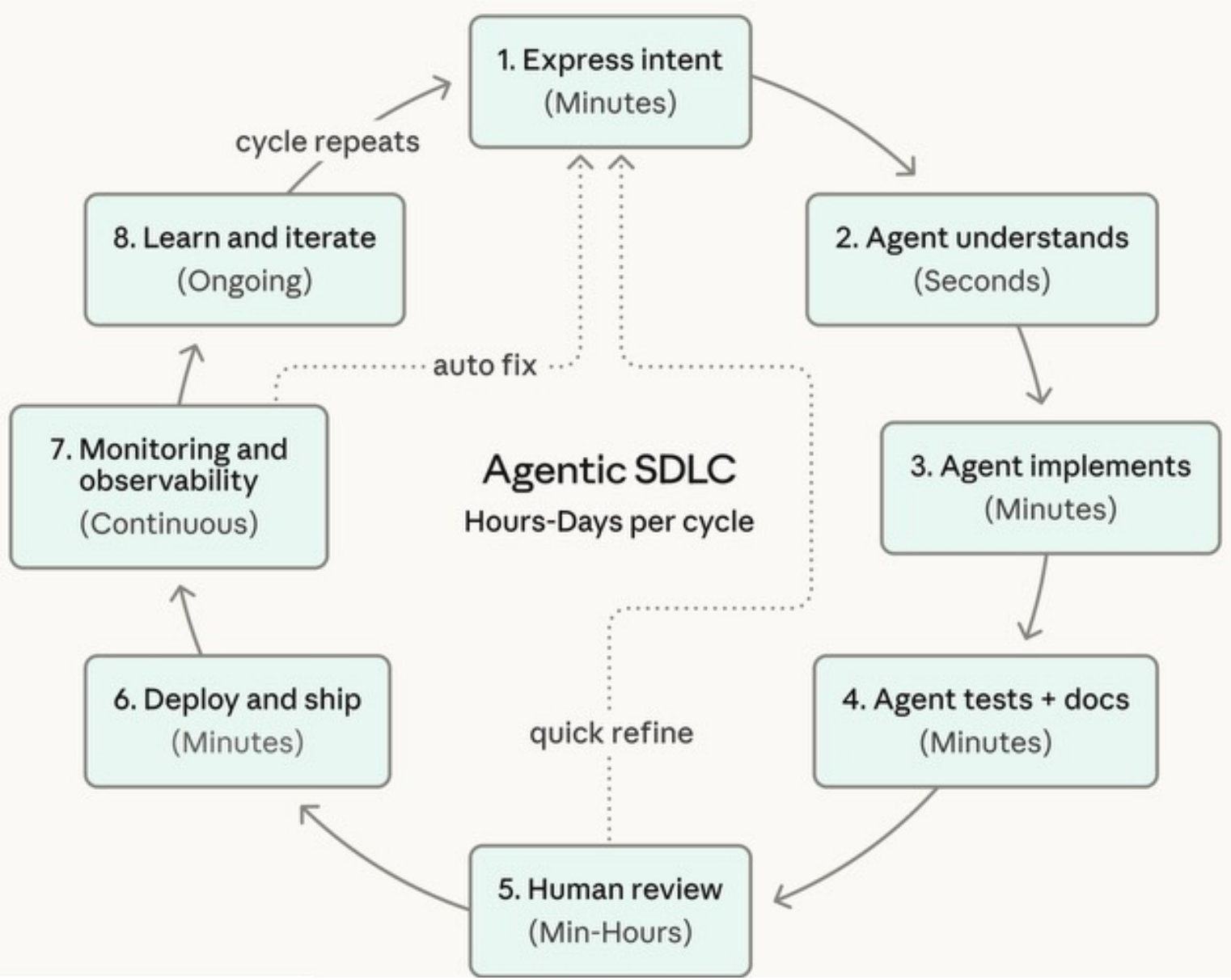
Connecting Multimodal GenAI
to Future AGI

Agentic Coding Software Development Lifecycle



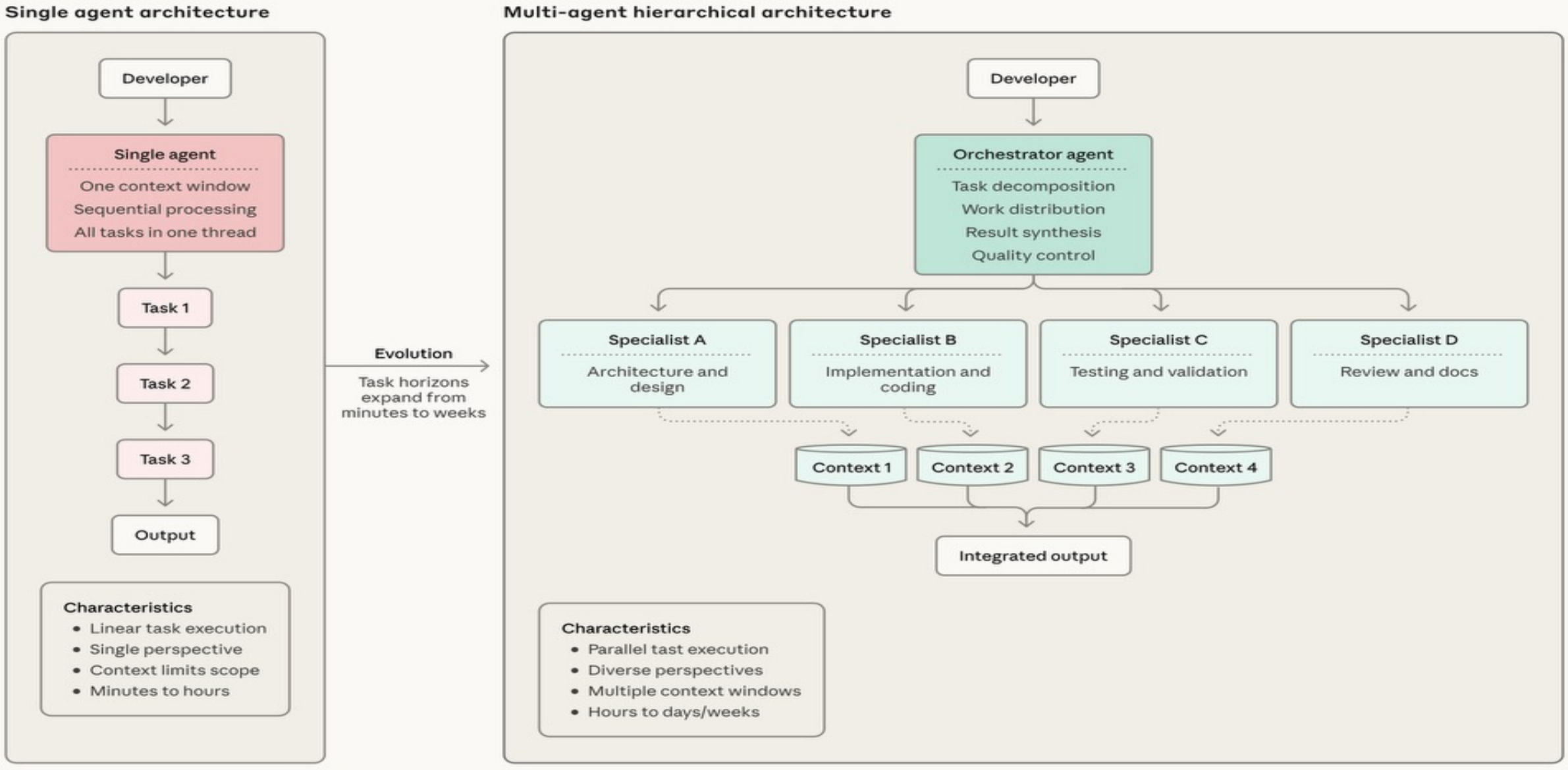
Source: Anthropic (2026), 2026 Agentic CodingTrends Report: How coding agents are reshaping software development, https://resources.anthropic.com/hubfs/2026%20Agentic%20Coding%20Trends%20Report.pdf

Agentic Coding Software Development Lifecycle



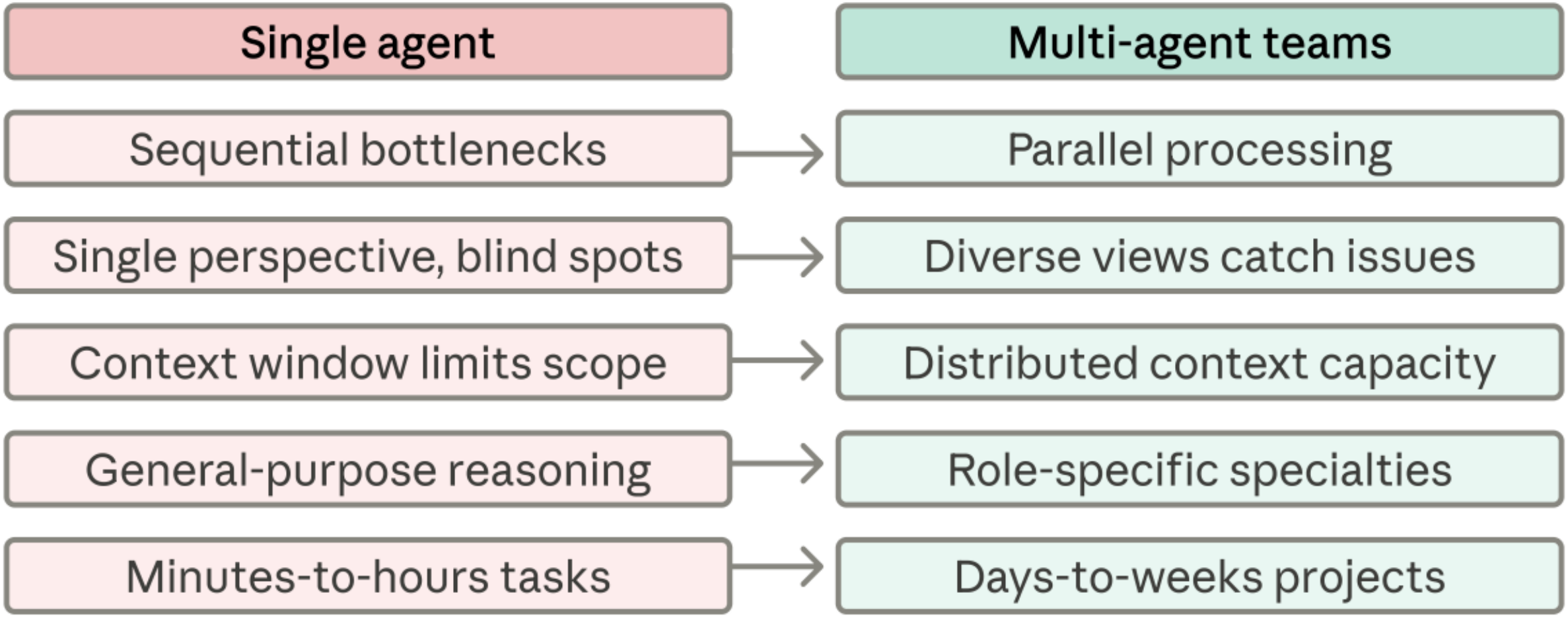
Source: Anthropic (2026), 2026 Agentic CodingTrends Report: How coding agents are reshaping software development, https://resources.anthropic.com/hubfs/2026%20Agentic%20Coding%20Trends%20Report.pdf

Coding Agent Architectures: From Single Agents to Coordinated Teams



Source: Anthropic (2026), 2026 Agentic CodingTrends Report: How coding agents are reshaping software development, https://resources.anthropic.com/hubfs/2026%20Agentic%20Coding%20Trends%20Report.pdf

Coding Agent Architectures: Single Agent to Multi-Agent Teams Performance Impact



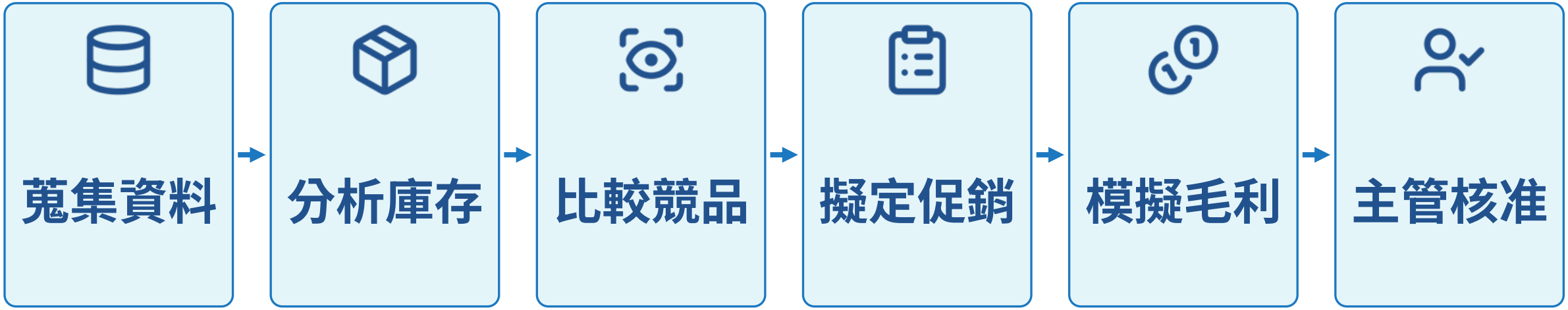
Source: Anthropic (2026), 2026 Agentic CodingTrends Report: How coding agents are reshaping software development, https://resources.anthropic.com/hubfs/2026%20Agentic%20Coding%20Trends%20Report.pdf

零售情境：從寫報告到完成任務

From Generative AI to Agentic AI

生成式 AI
撰寫市場分析報告

Agentic AI
取得授權後自行完成任務



主管核准後才執行

Why Agentic AI? Why Now?

2026 全球與臺灣關鍵數據

44%

McKinsey：
企業已擴展 AI

57%

LangChain：
Agent 已進入生產

33 家

臺灣金融業
導入代理式 AI

35.8%

臺灣商業服務業
已應用 AI

40%+

Gartner 預測：
專案恐被取消

Multi-Agent

臺灣經濟部政策方向

競爭焦點：流程重設、可靠性與治理

AI Agent、Agentic AI 與 Multi-Agent

概念定義

AI 類型	主要能力	商業例子
Predictive AI	預測、分類、評分	客戶流失預測
Generative AI	文字、圖像、程式生成	市場研究報告
AI Agent	目標導向、工具使用	處理例行訂單查詢
Agentic AI	規劃、決策、動態執行	跨部門訂單到交付
Multi-Agent	多代理分工、協調、驗證	行銷、財務、庫存協作

Agentic AI 核心能力

從「生成答案」到「使用外部系統完成任務」

Reasoning	推理與目標分解
Planning	任務規劃與動態修正
Tools	Function Calling 使用外部系統
Memory	RAG 知識檢索與工作記憶
Action	執行任務並回報結果

Agentic AI Reference Architecture

端到端系統架構

Human Goals & Governance
目標・授權・預算・審批

Agent Orchestrator
任務拆解・協調・狀態管理

Research Agent
檢索與知識

Analysis Agent
資料與推論

Action Agent
工具與執行

Enterprise Systems & Knowledge
LLM・RAG・MCP・API・ERP・CRM

Evaluation, Observability & Human Approval
資安・稽核・監控・人工審核

Agentic Workflow Design Patterns

Sequential、Parallel、Orchestrator



Sequential 順序式

步驟固定，逐步傳遞

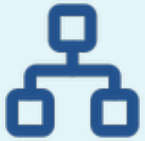
適用：報告生成



Parallel 平行式

子任務同時執行再整合

適用：多資料源檢索



Orchestrator 協調者式

動態拆解並指派任務

適用：開放式任務

先從最簡單可驗證的流程開始

MCP、A2A 與 Agent Interoperability

互通協定

MCP
Model Context Protocol
連接外部工具與資料
類比：AI 如何使用工具

A2A
Agent2Agent Protocol
代理之間傳遞任務
類比：代理如何溝通

A2A 已發展為 Linux Foundation 主導的開放協作計畫

Single-Agent vs. Multi-Agent

系統設計取捨

規則式工作流程
固定、可預測
簡單、便宜、可靠

單一 Agent
目標單一、工具有限
成本與可靠度易掌握

Multi-Agent
開放、跨領域任務
需控管協調成本

簡單 → 複雜

提醒：Multi-Agent 不是一律採用

Cross-Disciplinary Agentic AI Research

跨域研究全貌

多代理協作
任務分配與驗證

人機協作與信任
責任與決策權

領域專用代理
商學、財金、會計

代理評測
任務成效與成本

代理式流程創新
重設商業流程

可信任代理 AI
隱私、安全、稽核

Neurocomputing 2026 綜述六面向：
架構、認知、互動、可解釋、安全、評估

Multi-Agent Collaboration & Coordination

代理協作研究

研究面向

- 任務分配機制
- 辯論與交叉驗證
- 協調成本與錯誤擴散

研究提問

多代理協作是否真的比單代理更有效？

Human–AI Collaboration & Trust

人機協作研究

研究面向

- 信任校準
- 責任歸屬
- 決策權分配
- 使用者採納

研究提問

什麼任務由 AI 自主執行，
什麼任務必須有人審核？

Domain-Specific Agents & Knowledge

領域知識整合

研究面向

- 商學、財金與會計
- 醫療與法律專業
- 知識檢索與領域規則
- 準確性與可解釋性

研究提問

領域知識如何改善 Agent 的準確性與可解釋性？

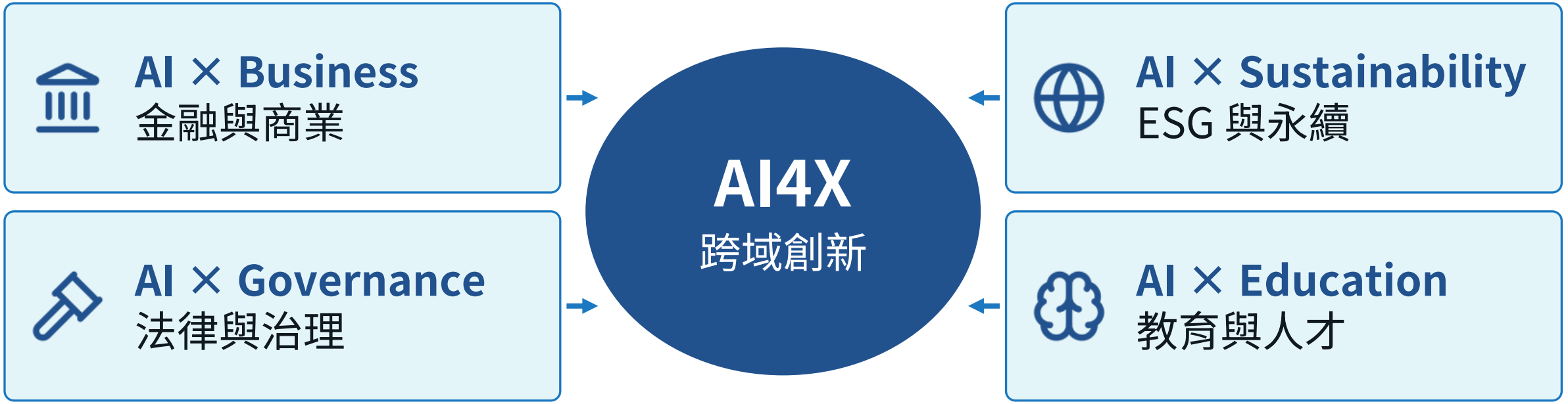
Agent Evaluation & Benchmarking

如何證明 Agent 真的帶來價值？

評估面向	建議 KPI
任務成效	Task Success Rate
品質	Accuracy、Citation Validity
效率	Execution Time、人工介入時間
經濟性	Cost per Task、ROI
安全性	Unauthorized Action Rate
可靠性	Recovery Rate、故障率
使用者採納	User Trust、Satisfaction

AI4X：AI for Cross-Disciplinary Innovation

跨域研究架構



跨領域知識 × 智慧代理 × 真實場域 × 可驗證效益

國立臺北大學 AI4X 研究中心：2026 年 8 月 1 日正式營運

https://ai4x.ntpu.edu.tw/

Agentic AI Industry Landscape

六大產業地圖

金融科技

研究報告與風險分析

零售行銷

客群洞察到策略優化

企業營運與供應鏈

訂單到異常預警

智慧製造

異常診斷與維修

教育科研

個人化學習輔導

ESG 永續

資料核對與報告

Agentic AI for Financial Services

金融應用趨勢

33 家
金融業已導入代理式 AI

15 家
其中為證券期貨業

主要應用

資料蒐集、研究報告撰寫與
程式碼檢核等內部作業

研究價值

金融資訊可信度・風險管理・
可解釋投資研究・合規

Multi-Agent Financial Research

金融研究案例與流程

情境：產生上市公司的投資研究草稿



人工把關：分析師審核來源與結論

應展示的價值指標

報告完成時間、資料正確率、引用完整度、人工修正次數、合規問題數

Agentic AI for Retail & E-Commerce

智慧商務應用

35.8% 已開始應用 AI

12.7% 已規模化使用



消費洞察



客群分析



行銷企劃



創意內容



績效分析



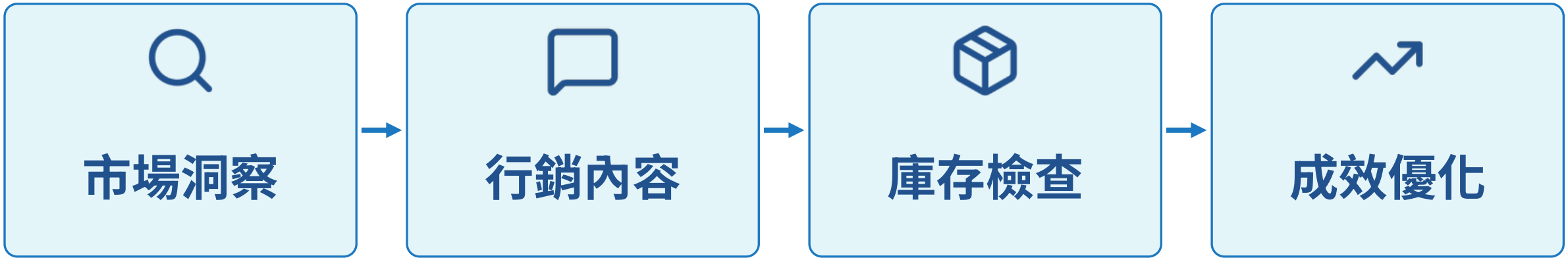
策略優化

研究價值：個人化行銷與行銷投資報酬

Marketing & Customer Experience Agents

智慧行銷案例

情境：中小型電商年度促銷活動



人工把關：行銷主管審核內容與預算後上線

應展示的價值指標

企劃時間、轉換率、廣告投資報酬、缺貨率、客訴率

Agentic AI for Enterprise Operations

企業營運應用

訂單預測 → 庫存檢查 → 供應比價 → 採購建議 → 交期協調 → 異常預警

研究價值
跨系統互通、流程最佳化

關鍵觀察
價值來自跨系統流程整合

先做 Agent PoC：重複、跨系統、需判斷的工作

Supply Chain Multi-Agent Collaboration

供應鏈案例

Supervisor Agent
任務拆解・協調・檢查

需求預測代理
訂單與銷售

庫存代理
水位與缺貨

採購代理
比價與建議

物流代理
交期與異常

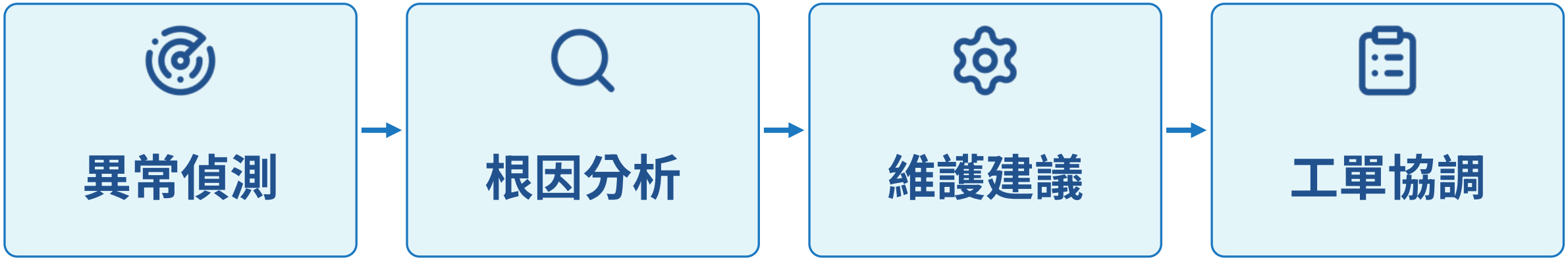
人工把關：採購人員核准後執行

建議指標：缺貨率、交期達成率、採購成本

Agentic AI for Smart Manufacturing

智慧製造案例

情境：製程品質異常



人工把關：工程師核准後，由受控系統執行

應展示的價值指標

異常處理時間、誤判率、停機時間、良率、每次處置成本

Agentic AI in Education & Research

教育科研應用

需求分析 → 教材推薦 → 學習輔導 → 練習回饋 → 教師覆核

個人化學習　教育公平　AI 素養　學術誠信

教師覆核是流程中的關鍵一環

Agentic ESG & Sustainability

永續金融與報告

ESG 資料蒐集	整合永續資料來源
碳排資訊核對	核對揭露內容
永續風險分析	評估風險與影響
報告草擬	代理協助撰寫初稿
專業查核	專業人員確認結論

研究價值：資料品質、資訊揭露、可信任 AI

現場展示：智慧商業研究助理

評估新產品的臺灣市場機會

使用者任務：評估環保隨行杯的臺灣市場機會，提出一頁式建議

Supervisor Agent
任務拆解、協調與檢查

市場研究 Agent

客群洞察 Agent

定價分析 Agent

策略報告 Agent

人工審核：檢查證據、假設與建議

Business Value & Agentic AI ROI

投資效益評估

工作是否正確完成
任務成功率
端到端完成率

成本是否可控
每任務成本
ROI

風險是否可接受
未授權行為率
資料外洩事件

Gartner 預測：2027 年底逾四成專案恐被取消

價值來自跨系統流程整合，而非漂亮的答案

Agentic AI Risks & Challenges

資安、隱私與可靠性

風險	問題	控制機制
幻覺與錯誤行動	錯誤資訊導致失誤	來源驗證、結構化檢查
Prompt Injection	惡意內容誘導越權	內容隔離、權限限制
資料與隱私	機密、個資外洩	最小權限、遮罩、稽核
Agent 連鎖錯誤	多代理錯誤放大	任務邊界、停止條件
成本與責任	反覆執行、成本失控	預算上限、人工核准

Agent Autonomy & Human Oversight

自主權分級

級別	角色	典型任務	建議控管
L0	提供建議	文字摘要	人工使用結果
L1	輔助分析	資料比較、草稿	人工審核
L2	受限執行	低風險資料更新	事前授權與紀錄
L3	條件式自動	指定範圍跨系統	金額門檻、例外升級
L4	高度自主	多代理動態協調	嚴格權限與中止機制

Trustworthy Agentic AI Governance

NIST、OWASP 與臺灣治理

NIST
2026 啟動
AI Agent 標準倡議
互通性與安全

OWASP
2026 Agentic 應用
Top 10
代理式系統安全

臺灣
《人工智慧基本法》
2025/12/23 三讀通過

可靠性必須先於自主性
治理是導入企業的必要條件

From AI PoC to Production

90 天實證流程

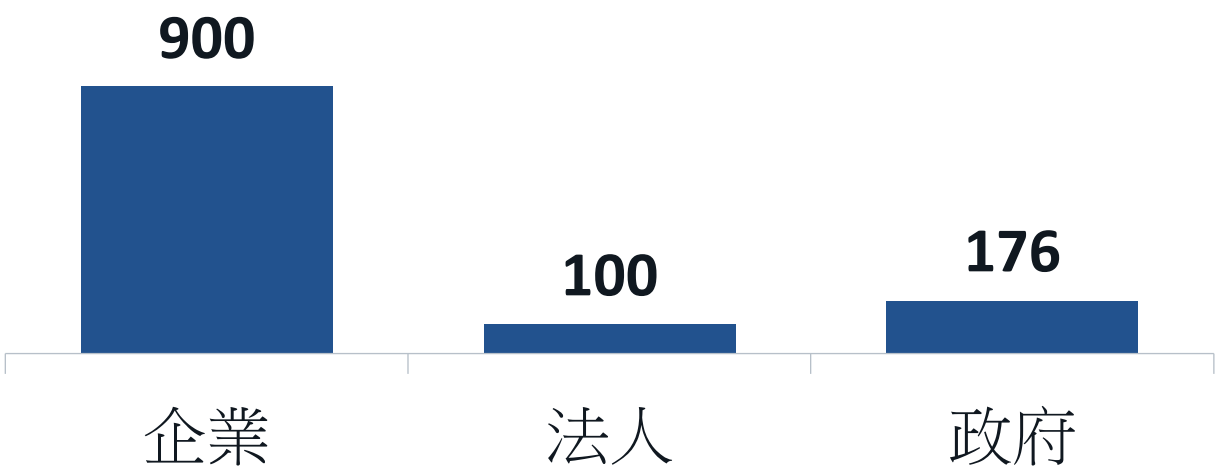
天數	階段	重點
Day 1–15	Problem Discovery	選定流程與基準
Day 16–35	Architecture Design	設計架構與審核點
Day 36–60	Prototype & Evaluation	以任務測試成效
Day 61–75	Controlled Pilot	受控場域試行
Day 76–90	Value Assessment	評估效益與擴展

NTPU AI4X 產學合作經驗總覽

Industry–Academia Collaboration

7	5	NT$ 11,760,000
合作計畫	合作單位	115 學年度合作經費

經費（NT$ 萬元）



企業合作
3 項｜900 萬

法人研究機構
2 項｜100 萬

政府計畫
2 項｜176 萬

https://ai4x.ntpu.edu.tw/zh/projects.html

NTPU AI4X 合作計畫地圖：七項計畫

Seven Collaboration Projects

類別	合作單位	計畫主題	經費
企業	康士藤顧問	AI 人資陪練與評量	300 萬
企業	崇越科技	AI 數位轉型教育訓練	500 萬
企業	綠創永續	循環材料、ESG 與 DPP	100 萬
法人	工研院	可信任 Agentic AI 智慧製造	70 萬
法人	工研院	開放網路 OCUDU 驗證	30 萬
政府	教育部	代理式 AI 課程（資管）	88 萬
政府	教育部	跨域 PBL 課程（社工）	88 萬

https://ai4x.ntpu.edu.tw/zh/projects.html

NTPU AI4X 經驗分析：Agentic AI 落地模式

合作計畫	對應研究方向
人資陪練與評量	人機協作與信任
數位轉型教育訓練	人才培育與導入
循環材料、ESG、DPP	Agentic ESG
可信任 Agentic AI 製造	領域知識與可信任
代理式 AI 課程	教育與人才

計畫在 12 個月內，適合 90 天 PoC

https://ai4x.ntpu.edu.tw/zh/projects.html

NTPU AI4X 已上線的 AI 平台

NTPU AI-Native Campus Platforms

NTPU AI

全校免費生成式 AI

AI Assistant

校園智慧問答

AI4X MCP

開放可追溯公開資訊

AI Learn

AI 工作力培育

Local Match

在地實作任務媒合

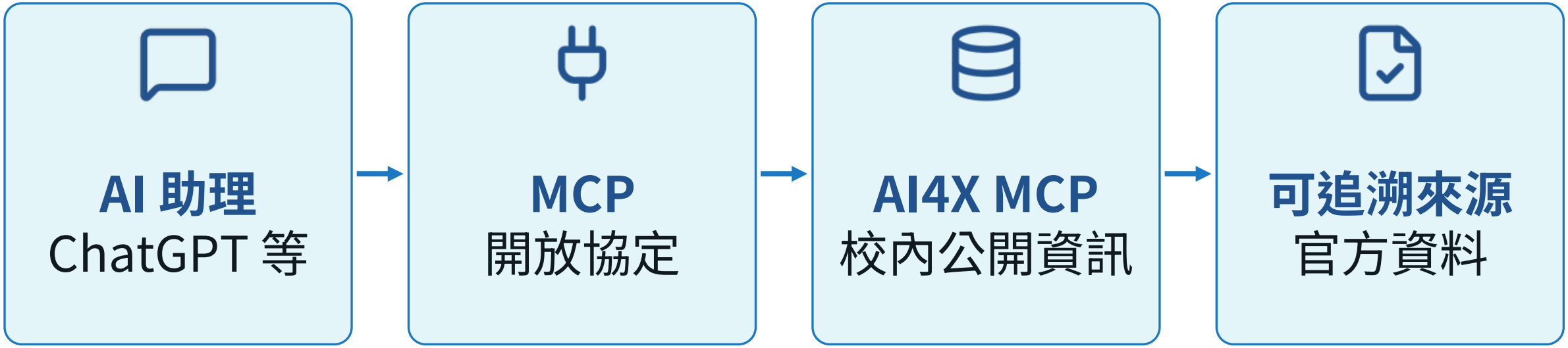
NAPAICP

競賽管理平台

https://ai4x.ntpu.edu.tw/zh/aiservices.html

MCP 實例：NTPU AI4X MCP

從協定到校園知識基礎設施



目前提供：研究專家・研究計畫・中心成員・服務・活動・公開文件

可信賴、可擴充的 AI 原生校園知識基礎設施

https://ai4x.ntpu.edu.tw/zh/aiservices.html

Agentic AI × University–Industry Collaboration

產學合作方向

項目	合作主題	可驗證成果
智慧金融	Agentic Financial Research	財金研究助理原型
智慧商務	Agentic Retail & Marketing	促銷與電商流程
智慧營運	Agentic Business Process	訂單、客服、供應鏈
永續創新	Agentic ESG Analytics	永續資料核對
智慧校園	Agentic Campus Services	校務知識服務

Building an AI4X Talent Ecosystem

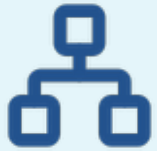
跨域人才培育



理解領域



設計流程



協調 Agents



衡量績效



管理風險

未來的 AI 人才，不只會使用 AI
更要能與 Agents 協作並管理風險

Agentic AI Outlook 2027–2028

前瞻研判，非已確定趨勢

個人 Agent	→	組織內 Agent Teams
單一企業工具	→	跨平台 Agent 互通
通用代理	→	具產業知識的專業 Agent
Demo 與 PoC	→	有評測與成本追蹤的生產級系統
人類操作所有步驟	→	人類設定方向與授權邊界

Key Takeaways

核心結論



AI Agents

改變工作的
執行方式



Agentic AI

改變企業的
流程與創新模式



跨域研究與治理

決定能否
創造永續價值

Open Discussion

教師與研究生

哪些研究流程
適合 Agentic AI？

企業與產學夥伴

哪些什麼工作
先做 PoC？

學生

應培養哪些能力？

Summary

1. AI 產業新典範：
   從回答問題到 Agentic AI 完成任務
2. Agentic AI 技術核心：
   Agent 架構與互通協定
3. 跨域研究前沿：
   研究問題與評測
4. 產業應用與國立臺北大學經驗：
   從情境到可驗證價值

臺北商業大學
AI產業趨勢講座

Q & A

Agentic AI 跨域研究與產業創新應用趨勢

Agentic AI Trends in Interdisciplinary Research and Innovative Industrial Applications

時間：2026/11/5 (四) 下午 12:00~13:30
地點：臺北商業大學 行政大樓7樓 第一會議室
主辦單位：國立臺北商業大學 研究發展處
(台北市中正區濟南路一段321號)



戴敏育 教授 (Prof. Min-Yuh Day)

國立臺北大學 資訊管理研究所 所長

跨域 AI 前瞻研究中心 (AI4X NTPU) 主任