DOI: 10.6653/MoCICHE.202510_52(5).0005

# 智慧型代理人於公共工程採購風險預警之應用

陳致霖*／國立屏東科技大學土木工程系 助理教授
薛文蔚／核桃運算股份有限公司 總經理

公共工程採購制度長期存在資訊分散、評估標準主觀及查核資源有限等挑戰，使得標案評選過程易淪為低價競標，忽略工程品質與治理效益，本研究嘗試導入大型語言模型（Large Language Models, LLM）驅動之智慧型代理人（AI Agent），建構公共工程採購風險預警平台，以期提升決策客觀性與查核效能，研究架構以 Llama3-TAIDE 模型作為智慧核心，並結合 Reflection、Tool Use、Planning 與 Multi-Agent 四大設計模式，支持自我反思迭代、多工具整合、任務規劃分解與跨代理協作，系統功能涵蓋短期與長期記憶維護、自然語言跨資料源檢索（採購紀錄、財報、職災資料等）、風險成本估算、查核排程與沉浸式數據探索介面，透過此平台預期可降低決策主觀性、提升公共工程品質與透明度，並促進工程管理朝向智慧化、數據驅動與永續治理之方向發展。

## 前言

傳統的公共工程採購制度中，工程類型多樣豐富，對於開標單位來說，每一次開標都對應著無數家的投標廠商，然而政府的查核資源相對有限，加上廠商資訊大多散落在不同平台當中，整合起來相對困難，通常會花費大量的時間與精力；此外另一個困境在於，政府單位評估相對主觀，導致選案缺乏一致性的標準，因此多數評選仍以報價為主要依據，缺乏對廠商財務穩定性、歷史履約表現、職災紀錄等面向的量化分析。對於投標廠商而言，則主要面臨政府資料龐大且零散的問題，即便可以在平台上查到與標案相關的公開數據，但資訊分散在不同平台，對於中小型廠商而言，缺乏全面資訊與歷史分析工具，使得投標策略往往淪落至「價格戰」以低價競標的惡性循環當中。這樣的結構性問題，使得開標單位在決策上，常陷於「資訊可得但無法用好」的困境，也讓投標市場長期停留在價格戰導向，忽略了工程品質與長期治理效益，如何在標案前快速掌握多方數據資訊成為雙方迫切的課題。

在公共工程管理中，工程品質查核是確保施工品質、落實契約規範的重要措施，主管機關透過查核程序，以客觀方式評定工程品質，進而督促監造單位與承包商強化品質管理，查核結果不僅可作為工程單位內部考評的依據，亦能提供廠商改善施工品質與遴選優良廠商的重要參考，目前工程查核作業中在實務應用中，因工程類型多樣、查核資源有限，以及資料評估的主觀性，導致選案缺乏一致性標準，藉由蒐集政府採購數據資料，結合人工智慧與大數據分析技術，可發展出一套客觀化的智慧選案決策模式，透過分析歷年查核結果、工程類型、標案金額、施工進度與異常事件等資料指標建構預測模型，以輔助主管機關於有限資源下進行查核案件之優先排序與選案判斷。因此旨在建立一套以資料驅動為基礎的智慧查核選案決策系統，提升查核效能、

* 通訊作者，waynechen@mail.npust.edu.tw

降低人為主觀判斷，並協助政策制定者在查核資源配置上作出更合理與有效的決策，最終達到提升公共工程品質與施工透明度的目標。

## 大型語言模型驅動智慧代理進展

隨著大型語言模型（LLM）的最新進展，基於LLM的人工智慧代理憑藉其強大的介面（能夠理解人類和機器語言）取得了突破性的進步，研究表明智慧代理人可以有效地建立虛擬模型、處理數據，並在數位孿生模型中與使用者無縫互動，打破以往需翻閱冗長報表才能取得資訊的瓶頸[1-5]，此亦為工程領域發展之重點趨勢[6-8]。

有關智慧型代理人（AI Agent）《The 2025 AI Agent Ecosystem v2》（來源：Jeremiah Owyang, Blitzscaling Ventures, 2024年9月）報告趨勢指出可分為四大層級（如圖1所示），資料層是所有AI Agent運作的基礎，透過私有資料庫（如企業內部監測數據、個人隱私資訊）與公開資料源（政府開放資料、第三方API）相結合，並依靠統一API介面確保存取效率與合規性，為上層算法提供豐富且可信的訓練與推理素材。管理層則肩負維繫整體生態安全與穩定運行的重任，透過KYA（Know Your Agent）驗證、分級憑證、AgentOps監控、網路仲裁及自我修復機制，確保每一位代理在各自邊界內行動，並能在發生異常時迅速回滾或隔離風險；應用層進一步將這些代理技術落地轉化為可視化、可互動的解決方案，既有無程式碼平台讓業務人員輕鬆配置多通道客服或數據分析Agent，也有專業SDK與開源框架支持研發者打造客製化智能機器人，並且未來將透過動態生成機制自動產生新應用、快速迭代；最外層的生態系市場則由亞馬遜、谷歌、微軟等巨頭與眾多新創共同競爭與協作，為各式場景提供「即插即用」或「按需訂閱」的代理服務，推動企業與個人用戶進入AI原生時代。四層相輔相成，不僅形成完整的技術到商業化閉環，也將使AI Agent成為未來互聯網、行動應用及企業軟體的核心動力，引領跨產業跨域的智慧化轉型浪潮。

## 整體架構與功能

在架構開發上本研究以財團法人國家實驗研究院開發「Llama3-TAIDE模型」作為LLM智慧核心，TAIDE能提供70億參數之大型語言模型，並融入臺灣特有的語言、價值觀、風俗習慣等元素，使生成式AI引擎能夠更好地理解和回應在地使用者的需求，具備可信任的生成式AI引擎基礎模型，並應用於不同領域，以滿足使用者多元化的需求。此模型支持複雜任務的自主決策與執行，前端開發則採用Google的Angular框架，構建跨平台且用戶友善的介面，確保良好的互動體驗，後端方面使用Python 3.10+負責邏輯處理、強化學習演算法與模型整合；Node.js 18+則負責實作API閘道，並與Angular前端框架進行串接，為提升系統的可擴展性與穩定性，採用Docker進行容器化，並以Kubernetes實現彈性部署與資源管理，確保智慧代理服務能穩定高效運行，滿足政府採購預警平台之需求。

本研究整體系統分為多個關鍵模組，如圖2所示。在Memory模組中，系統同時維護短期記憶與長期記憶，將用戶交互資訊、採購與財報資料、職災紀錄及歷史查核決策持久保存，為後續推理提供豐富上下文；Planning模組負責接收當前狀態，利用子目標分解（Subgoal Decomposition）與思考鏈（Chain of Thoughts）策略，結合自我批評（Self-critics）與反思（Reflection）機制，持續優化維護行動計劃；在Tools模組中，系統整合了OpenRAG技術，使使用者可透過自然語言即時查詢，跨越多個資料來源（如採購紀錄、財務報表與職災資料

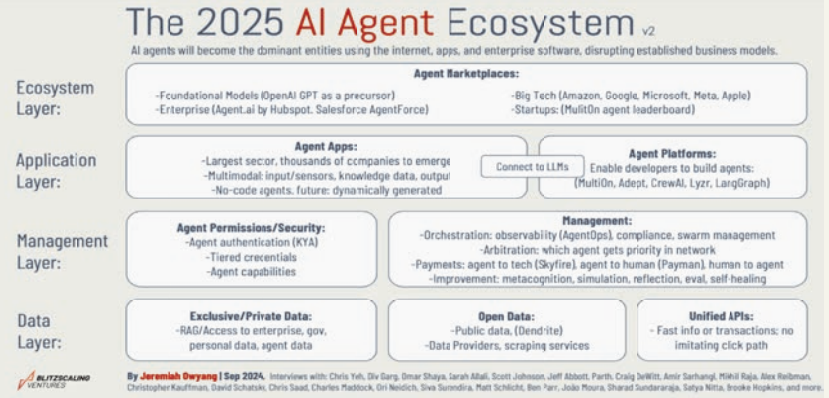


圖1 The 2025 AI Agent Ecosystem發展框架[9]

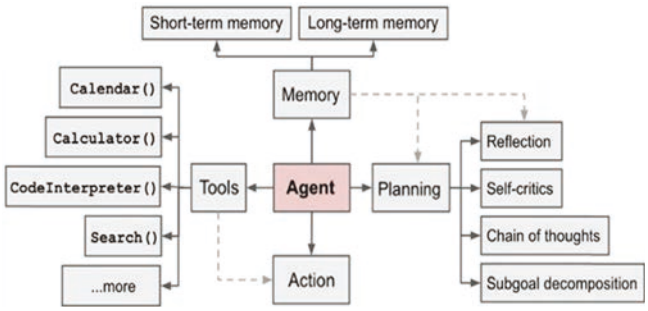


圖 2　本研究 AI Agent 開發框架

自動獲得整合答案，顯著降低對傳統 SQL 查詢與原始數據處理的依賴，並提升查詢效率與可用性。同時，Agent 亦能調用多種工具，包括 Calendar ( ) 進行查核排程、Calculator ( ) 做成本與風險估算、CodeInterpreter ( ) 進行動態程式運算，以及 Search ( ) 以擴充資料檢索能力；最後，Action 層將規劃結果轉化為具體的 API 請求或使用者指令，並通過前端儀表板或表單直觀呈現分析結果。此架構透過前端畫面 Angular 與 OpenAI API 的緊密整合，不僅保障跨平台操作流暢，也具備高度擴展性、自動化且可追溯的智慧 Agent 解決方案。

在 Agent AI 及其關鍵設計模式中，理解每種模式如何賦能大型語言模型（LLM），使其具備更高自主性與效能至關重要。本研究透過大型語言模型（LLM）之四大智慧代理設計模式 Reflection Pattern、Tool Use Pattern、Planning Pattern 以及 Multi-Agent Pattern 四種先進的政府採購風險 AI Agent，各功能流程敘述下：

1. Reflection Pattern（反思模式）– 在本系統中反思模式是核心驅動機制，AI Agent 能根據最新採購紀錄、財報數據與職災資料，不斷進行自我評估與迭代修正，避免錯誤推論的累積，透過反思與再生成過程，系統能持續優化風險辨識模型與決策結果，並於沉浸式視覺化介面中即時更新，讓查核人員直觀理解數據背後的推理邏輯。此模式亦能促進模型的持續學習，使系統隨著時間演進自我完善，強化長期運作的穩定性與適應性。
2. Tool Use Pattern（工具使用模式）– AI Agent 能靈活調用多元工具與數據來源，並透過 OpenRAG 技術，使查核人員僅需輸入自然語言，即可自動檢索並整合跨資料源資訊（如採購星球、財報星球、職災星球）。同時 Agent 亦可調用 Calculator ( ) 進行風險成本估算、Calendar ( ) 規劃查核排程，以及 CodeInterpreter ( ) 執行動態分析，多工具整合大幅降低對傳統 SQL 與原始資料處理的依賴，提升使用者體驗與查詢效率。
3. Planning Pattern（規劃模式）– AI Agent 能將複雜的採購查核或風險辨識流程拆解為多個子任務，並依據查詢回饋與最新資料動態調整行動計畫。舉例而言，當查核人員查詢「該廠商是否具備高風險特徵」時，系統會自動分解為子目標：(1) 搜尋歷年得標紀錄、(2) 分析財務異常、(3) 比對職災紀錄，最後在視覺化介面中合併呈現結果，提升查核透明度與決策精準度。
4. Multi-Agent Pattern（多代理人模式）– 系統中配置多個專業代理人分工協作，例如「採購紀錄代理人」、「財報分析代理人」、「職災風險代理人」等。這些代理人彼此共享資訊並協同決策，模擬跨部門查核團隊的合作模式。最終結果將在沉浸式數據探索介面中進行關聯視覺化，幫助使用者快速掌握全貌，並支援不同查核場景下的即時決策需求。

## 應用場景與情境

公共工程涉及龐大的資金投入與高度社會關注，任何施工品質不良、廠商違規或財務風險，都可能導致工程延宕、追加預算，甚至影響公共安全。然而，過去查核人員在審查過程中，往往需要手動蒐集不同來源的數據，如政府採購紀錄、廠商財報、職災通報等。這些資料分散於不同系統，格式不一，且查詢門檻高，導致查核效率低落、風險難以及時發現。基於此，本研究透過 AI-Ready 開放資料生態系與 OpenRAG 技術，打造沉浸式數據探索與智慧型代理人輔助平台，如圖 3 所示。查核人員僅需以自然語言輸入問題，系統即可即時整合採購星球、財報星球與職災星球等資料，並在 AI Agent 的協助下，快速完成風險辨識與決策支援，應用情境說明如下：

1. 查核人員進行標案資格審查 – 當政府單位要核准某廠商承攬大型公共工程時，查核人員可透過自然語言輸入：「請檢查該廠商近五年的得標紀錄與是否曾有職災通報。」AI Agent 會自動調用採購星球資料庫，列出該廠商的歷年標案紀錄；再串接財報星球，檢測是否存在資金缺口或債務異常；最後比對職災星球，檢視是否有多次重大職業災害。結果將即時呈現，協助查核人員快速判斷該廠商是否具備承攬資格。
2. 異常預警與主動通知 – AI Agent 不僅被動回應查詢，還能主動監測資料異動。例如，若某承包商的財報出現異常虧損或債務暴增，AI Agent 會自動推播警訊給相關查核人員，並附上數據佐證，提醒其注意潛在風險，避免不良廠商進入公共工程市場。


圖 3　智慧型代理人之公共工程採購風險預警平台開發情境應用

3. 工程執行期間的風險追蹤 – 在公共工程施工過程中，風險並非只存在於標案審查階段，而是會隨著工程進度持續變動。因此本研究所設計的 AI Agent 能在工程執行期間，持續監控承攬廠商是否涉及新的違規案件或職業災害。例如，若工地在施工過程中發生重大安全事故，AI Agent 可即時串接職業安全衛生署（職安署）的公開資料，並將最新的事故通報、違規裁罰或罰鍰紀錄，整合至系統平台中，這些資訊會自動更新至廠商風險評級，使查核人員與監管單位能第一時間掌握風險狀況此外，AI Agent 也能透過週期性資料比對與不定時更新機制，自動追蹤相關資訊。例如：查核人員可進一步透過自然語言詢問：「該廠商近一年是否有重複發生相同類型的職災？」系統即可即時回覆並給出具體數據依據。
4. 查核人員沉浸式探索情境 – 傳統查核多為靜態報表比對，本研究的沉浸式數據探索介面，讓查核人員能以互動方式瀏覽不同維度的資訊。例如，他們可以在 3D 知識圖譜中點擊某廠商節點，即時展開其關聯的得標紀錄、財報異常、職災事件。AI Agent 則像「智慧助理」般解釋數據意涵，並回答「該廠商是否與其他違規廠商存在合作關係？」等進階問題，提升探索的直覺性與深度。

## 結論

本研究針對公共工程採購過程中資訊分散、評估主觀與查核資源不足等問題，提出以大型語言模型（LLM）驅動之智慧型代理人應用架構，建構公共工程採購風險預警平台，應用層面上該平台能協助主管機關於標案資格審查、異常預警通知、施工期間風險追蹤及跨部門查核決策等場景中，快速掌握廠商風險全貌，並合理分配有限查核資源。此舉不僅能提升查核效能與決策透明度，也有助於改善低價競標導向的結構性問題，進一步強化公共工程品質與社會信任，本研究驗證了智慧型代理人在公共工程採購風險管理中的可行性與價值，為未來推動數據驅動之智慧治理模式奠定基礎。

## 參考文獻


1. Choi, S. and Yoon, S. (2024). GPT-based data-driven urban building energy modeling(GPT-UBEM): Concept, methodology, and case studies. Energy and Buildings, 325, 115042. https://doi.org/10.1016/j.enbuild.2024.115042
2. Huang, Y., Zhang, J., Chen, X., Lam, A. H. F., and Chen, B. M. (2024). From Simulation to Prediction: Enhancing Digital Twins with Advanced Generative AI Technologies. 2024 IEEE 18th International Conference on Control & Automation (ICCA), 490-495. https://doi.org/10.1109/ICCA62789.2024.10591881
3. Hwang, J. and Yoon, S.(2025). AI agent-based indoor environmental informatics: Concept, methodology, and case study. Building and Environment, 277, 112879. https://doi.org/10.1016/j.buildenv.2025.112879
4. Sun, Y., Zhang, Q., Bao, J., Lu, Y., and Liu, S. (2024). Empowering digital twins with large language models for global temporal feature learning. Journal of Manufacturing Systems, 74, 83-99. https://doi.org/10.1016/j.jmsy.2024.02.015
5. Yoon, S., Song, J., and Li, J.(2025). Ontology-enabled AI agent-driven intelligent digital twins for building operations and maintenance. Journal of Building Engineering, 108, 112802. https://doi.org/10.1016/j.jobe.2025.112802Abioye, S. O., Oyedele, L. O., Akanbi, L., Ajayi, A., Davila Delgado, J. M., Bilal, M., Akinade, O. O., and Ahmed, A. (2021). Artificial intelligence in the construction industry: A review of present status, opportunities and future challenges. Journal of Building Engineering, 44, 103299. https://doi.org/10.1016/j.jobe.2021.103299
6. Hosseini, S. and Seilani, H. (2025). The role of agentic AI in shaping a smart future: A systematic review. Array, 26, 100399. https://doi.org/10.1016/j.array.2025.100399
7. Siemon, D., Strohmann, T., and Michalke, S. (2022). Creative Potential Through Artificial Intelligence: Recommendations for Improving Corporate and Entrepreneurial Innovation Activities. https://lutpub.lut.fi/handle/10024/163914
8. 國科會土木水利學門
9. Owyang J. (2025, September 20). 2025: AI Agent Ecosystem. Jeremiah Owyang | Tech+Business. https://jowyang.beehiiv.com/p/2025-ai-agent-ecosystem