白皮書

歡迎來到思考型工廠

AI 如何為 MES 賦予大腦

作者：Francisco Almada Lobo
CEO at Critical Manufacturing

Critical manufacturing
an ASMPT company

目錄

執行摘要

製造業正在進入新時代,智慧不再局限於孤立的演算法或分析儀錶板,而是融入作業系統本身。在此脈絡下,自動化、MES(製造執行系統)與資料平台之間的傳統界限逐漸消失。取而代之的是導入AI的統一架構,不僅能協調生產,還能自主推理、適應和改進。

本白皮書探討實現此轉型所需的技術和組織變革。文中提出「思考型工廠」的概念,這是一種以數位方式整合的自我學習環境,以自動化、MES與資料架構之間的核心綜效為基礎。此外,也概述次世代AI(從傳統機器學習到大型語言模型(LLM),再到以代理程式為基礎的系統)如何仰賴更智慧化的模型,以及更智慧化的基礎架構。

如果缺少將作業、執行與脈絡連結的基礎資料模型,即使是最先進的AI解決方案也只會是零散、無法發揮最大效益的工具。本文的目的是讓決策者和數位轉型領導者瞭解此基礎的重要性、樣貌以及如何從策略著手,將AI定位成製造業大腦的原生層,而不是附加功能。

> 「到2029年,電腦將擁有情商,
> 並像人一樣具有說服力。」
>
> **Ray Kurzweil**

智慧製造的時代

Ray Kurzweil 對於指數級技術變革的預測不再只是理論。在製造領域，此變革正隨著自動化、人工智慧和連線能力快速進步而顯現。

工業革命在過去歷經數十年，而如今在資料、演算法和運算能力的聚合推動之下，我們在短短幾年內就已目睹典範轉移。

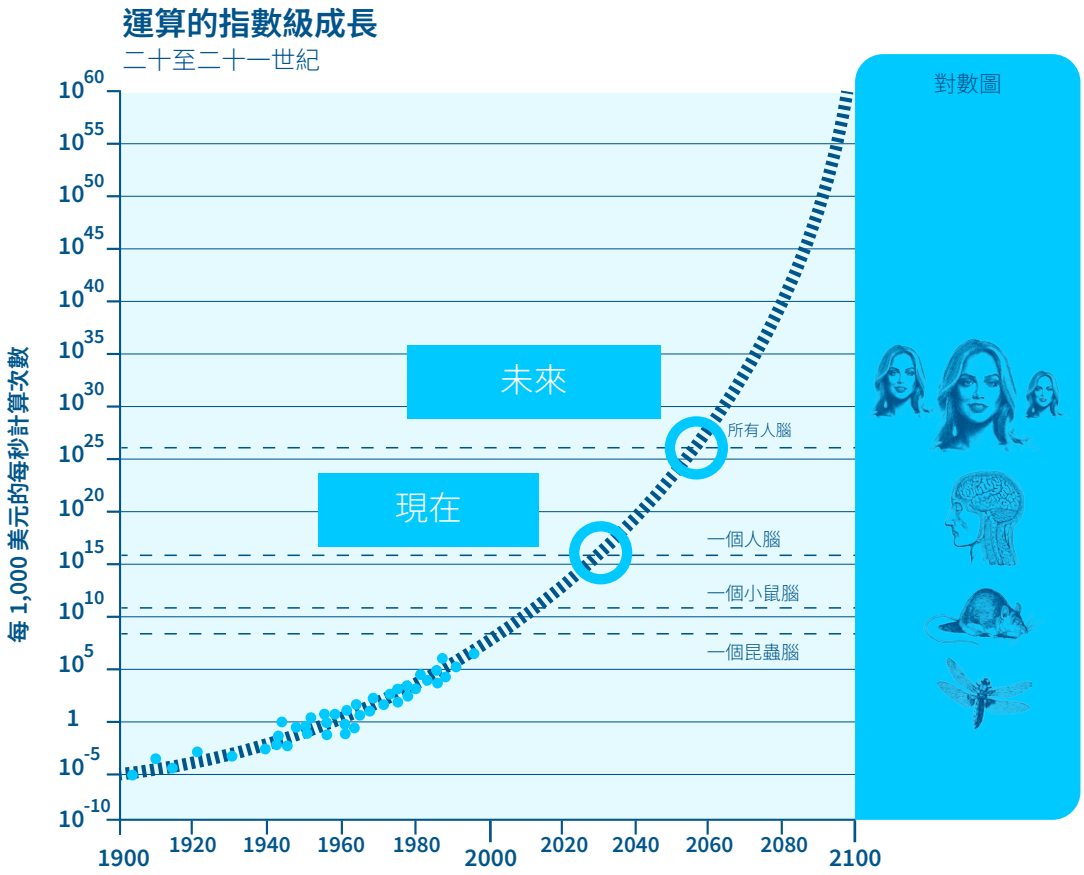

圖1：運算的指數級成長

來源：The Singularity is Near，Ray Kurzweil，2005年

工業領域正處於「思考型工廠」的轉折點。機器不僅執行命令，也開始理解脈絡、從規律中學習並即時調整其行為。GPT-4、Claude 3等LLM（大型語言模型）展現在過去被認為只有人類操作員才具備的複雜推理能力。多代理程式系統讓分散式系統得以協作，朝目標邁進。但在許多工廠現場，現實仍被僵化的規則、孤島化資料和狹隘的自動化邏輯支配。

訊息很明確：轉型勢在必行。在AI成為優秀操作員的世界中，快速適應的能力不再是競爭優勢，而是生存的必要條件。

製造業適應差距

雖然有眾多技術可能性,但大多數製造商仍未為未來做好準備。這是因為Scott Brinker提出的Martec定律:技術呈現指數級變化,但組織呈現對數級變化。

結果是出現適應差距,技術可能性與實際執行的之間的距離越來越大。

Martec 定律和適應差距

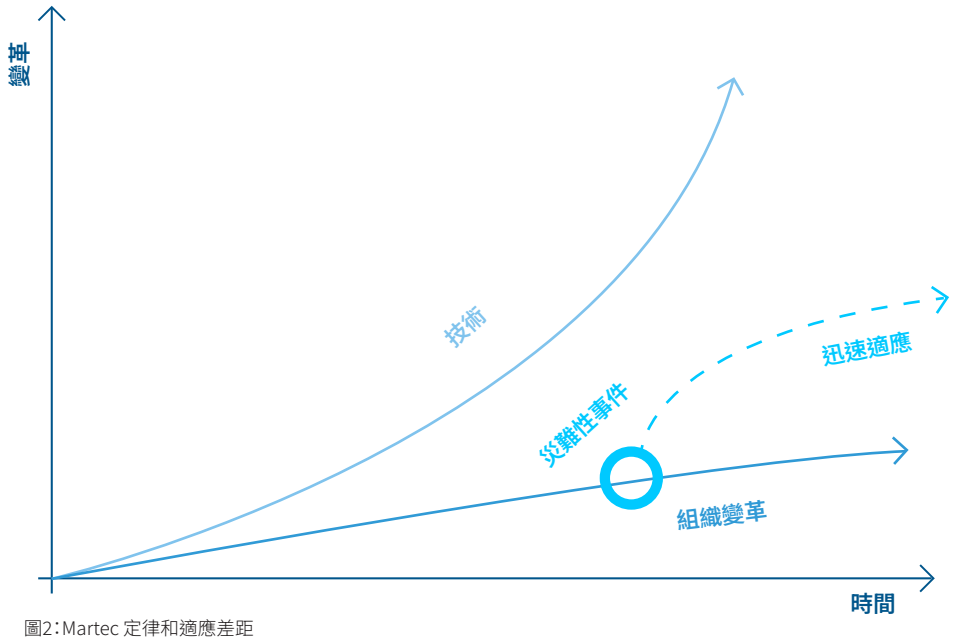

圖2:Martec 定律和適應差距

因此,在21世紀不會經歷100年的進步,而是接近20,000年的進步 (以現在的速度)。
Ray Kurzweil (2001)「The Law of Accelerating Returns」

傳統MES系統從來就不是為了智慧即時推理而設計。它們以固定邏輯運作,需要手動配置,也無法原生擷取非結構化資料,例如紀錄、影像或文字。AI和資料科學團隊往往孤島化,與維持現場運作的系統分離。工具零散化。資料不完整或不一致。結果是什麼?AI先導計畫或許在單獨運作時展現潛力,但無法在生產中規模化。

這不僅是技術問題,更是架構問題。問題在於分層思考,但若要利用此機會,需要會思考的系統。如果MES、自動化與資料平台仍維持鬆散耦合,AI就會淪為外圍的配角,而不是中樞神經系統。

製造業AI的基礎:資料、MES與自動化

製造商必須先將其數位核心現代化,才能利用先進的AI模型。首先要整合三個基礎要素:自動化、MES和資料平台。自動化產生即時訊號,反映生產的實際狀態。MES提供作業脈絡並管理製程邏輯。資料平台儲存並公開結構化和非結構化資料,以供分析使用。

這些要素構成「智慧製造的三位一體」。唯有以共同資料模型為中心來協調三者,下游AI功能(例如預測品質、智慧排程或AI代理程式)才能可靠地運作。架構良好的MES和資料平台堆疊不僅提供作業資料,也提供AI有效推理所需的語意脈絡。如果少了此脈絡,傳統機器學習模型的範圍仍然淺薄、狹隘,生成式AI模型(例如LLM)則與它們應該支援的真實環境脫節。在此情況下,由於缺乏結構化作業資料的基礎,LLM可能會產生幻覺、誤解輸入或做出不可靠的決策。

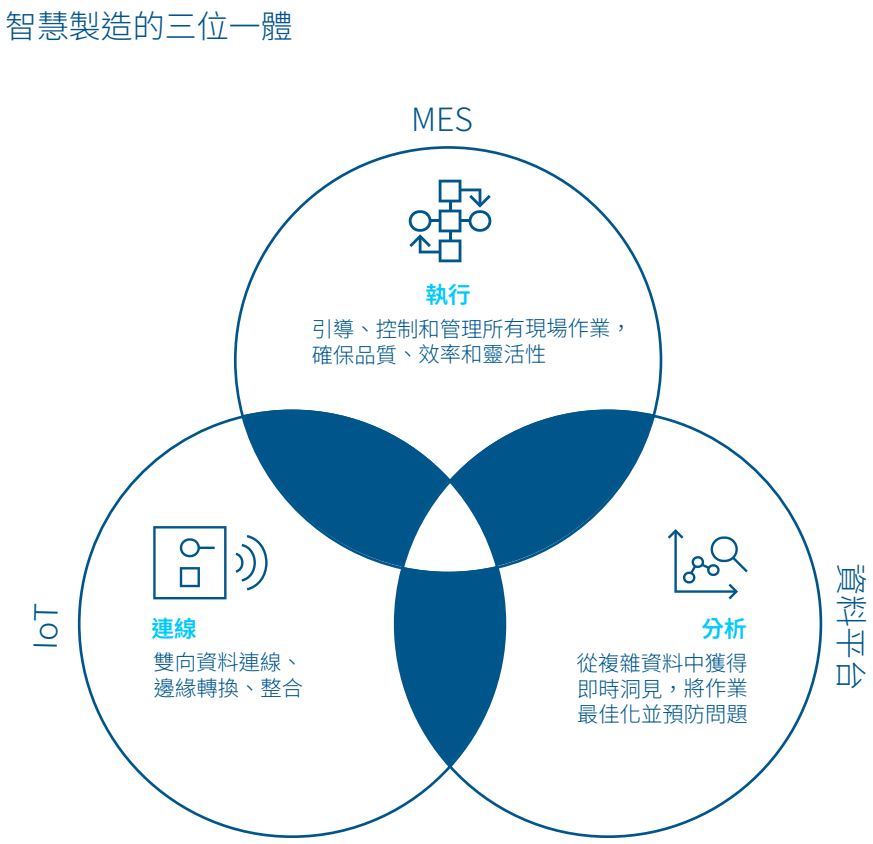

圖 3:智慧製造的三位一體

從ML到LLM,再到代理程式:三波AI浪潮

製造業人工智慧並非一成不變的,而是不斷演變的光譜。瞭解其進展有助於解釋過去的努力為何不如預期,以及新的模型為何具有潛力。

可從三個重疊卻又截然不同的AI浪潮來理解發展軌跡:傳統機器學習、LLM和AI代理程式。

三波 AI 浪潮

圖 4:三波 AI 浪潮

第一波是傳統ML,實現以結構化資料和統計學習為基礎的預測模型。這些系統可預測需求、維護需求或偵測異常,但它們需要純淨的輸入和大量的人工監督。

第二波是LLM,開創跨自然語言和非結構化領域的通用智慧。這些經過龐大語料庫訓練的模型可彙整紀錄、草擬 SOP,並以淺顯易懂的語言與操作員互動。但它們在領域基礎、幻覺和運作可靠性方面仍顯不足。

第三波是AI代理程式,將LLM功能與記憶、規劃和工具使用結合。這些代理程式可採取行動、根據回饋而調整,並跨步驟進行推理。它們不僅可回答問題,還能解決問題、啟動工作流程並跨系統協作。在製造業,此演變將智慧帶到帶到了最靠近現場的地方。

LLM 在工廠現場的前景

如果謹慎使用，LLM將擁有極大的工業應用潛力。它們具備語言理解能力，可以透過直覺、對話式的介面，將過去各自獨立的職能部門，如工程、營運、維護和 IT，連接起來。

主要前景

- **自然語言介面：**操作員或工程師可提出問題，例如「昨天良率下降的原因是什麼？」或「顯示3號生產線的維護趨勢」，並獲得有用的洞見。
- **自動化文件：**可即時產生或彙整SOP、工作指令、班次交接紀錄和例外報告。
- **根本原因探索：**與結構化紀錄或時間序列資料搭配時，LLM可協助進行初步診斷或異常分類。
- **跨系統推理：**可從MES、ERP、設備資料來源和PLM系統中擷取知識以統整洞見，不需要客製化儀錶板或自訂分析工具。

LLM不需要重新訓練即可跨領域運作，相較於傳統ML，部署速度更快，成本也更低。它們能以過去無法實現的規模進行實驗和迭代。但能力伴隨著風險，尤其是應用在重視安全或合規性的環境時。

缺陷:為何LLM在缺少結構的情況下會面臨困境

LLM雖然強大,但並非萬能的解決方案。其行為由機率驅動,而不是確定性。如果與即時結構化資料分離或未妥善部署,LLM可能會產生危險或誤導性的輸出。

幻覺:LLM可能產生看似合理,但完全錯誤的陳述。在製造業,這可能導致不正確的診斷、不安全的建議或不準確的文件,尤其是在輸出無法追溯至來源資料的情況下。

金魚腦:LLM沒有長期記憶。它們無法長時間保留脈絡,從一個班次、一天或一週獲得的洞見、異常情況或操作員偏好都會遺失,除非手動重新導入。因此難以維持連續性,尤其是在排除一再發生或不斷演變的問題時。

本末倒置:LLM可提出建議,例如「重新安排此工作」或「調整檢查頻率」,但它們不會執行,也不會說明如何在作業系統中執行這些行動。這導致智慧與行動之間脫節,造成瓶頸而非自動化。

如果在缺少結構化框架的情況下部署,這些限制會使LLM變得不可靠。更糟的是,它們的流暢性往往掩蓋易錯性,導致使用者在沒有深厚的領域知識或驗證機制的情況下難以判斷輸出是否可靠。

LLM症候群

圖 5:LLM症候群

讓LLM專業化並變得穩定的技術

為了克服這些缺陷,出現一些輔助技術。它們有助於調整LLM行為以符合特定領域需求,並讓模型以經過驗證的脈絡為根據,以降低風險。

檢索增強生成(RAG):RAG將LLM連線至可信的外部知識庫,通常是根據手冊、紀錄或結構化資料來源而建立的向量資料庫。就MES應用而言,這可能包括 MES文件、歷史MES資料、脈絡生產規則或組態檔。

微調:微調是指使用經過挑選的特定領域資料來訓練LLM,例如MES事件紀錄、組態資料或附有註解的操作員介入。這改善模型在重複性任務和技術語言上的表現,為製造作業提供更高的可靠性。

提示工程:提示工程是指設計精準的指令、範例或範本以引導LLM的行為,而不修改模型本身。這可能包括SOP範本、結構化查詢提示,或針對MES的問答範例。

這些技術使LLM在製造業中更具操作實用性。但真正的轉型需要可啟動、規劃、行動和適應的系統:AI代理程式。

將 **LLM** 專業化的方法

圖6:將LLM專業化的方法

AI 代理程式和代理工作流程的興起

LLM提供智慧建議,但它們基本上仍是無狀態且被動的。它們等待提示,提供回應,然後就忘記剛才發生的事。在製造業,這樣是不夠的。

製造業需要的是不只會解讀,還能規劃、行動、學習和協作的系統。這就是從LLM到AI代理程式的進步。

大腦、記憶和工具:**AI** 代理程式內部

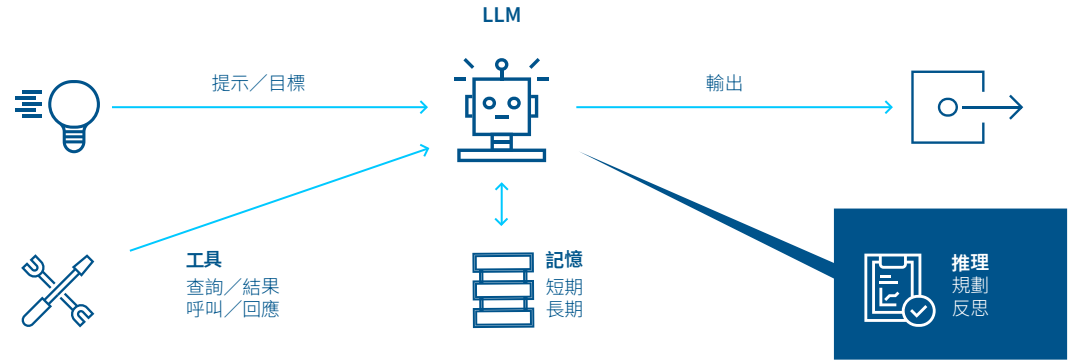

圖 7:大腦、記憶和工具:AI 代理程式內部

AI代理程式是有目標、使用工具與外界互動、保留記憶,並運用推理來達成目標的系統。

在MES中,由代理程式驅動的工作流程可應對動態輸入,例如生產條件變化或設備故障。它們可重新安排作業、重新規劃物料路線並將決策最佳化,而不仰賴硬編碼規則。

代理工作流程

圖8:代理工作流程

AI代理程式

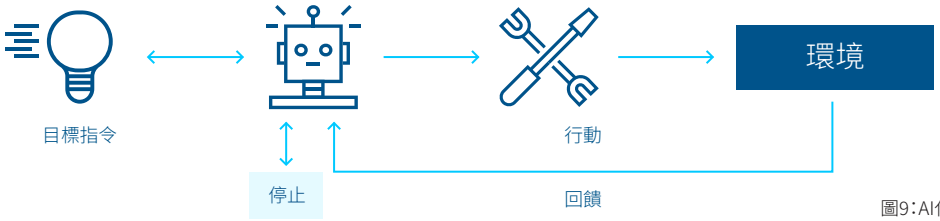

圖9:AI代理程式

有別於遵循線性、確定性流程的傳統MES邏輯,代理工作流程以條件式邏輯和推理來運作。

這造就更高的靈活性和韌性,這些是次世代MES系統的主要特性。

模型上下文協定 (MCP):MES中的AI基礎架構

隨著代理程式增加和專業化,它們需要以一致的方式與MES系統通訊、存取資料和共用脈絡。模型脈絡協定 (MCP) 是滿足此需求的基礎架構。

MCP提供的框架允許代理程式探索可用的API、存取共用記憶體,並且安全地與MES和資料平台通訊。它包含嵌入於每個代理程式中的MCP用戶端,以及公開MES物件 (例如物料、排程和品質參數) 的MCP伺服器。

透過MCP,代理程式能以模組化方式運作,不必針對每個功能進行自訂整合。它將互動標準化,並讓代理程式能被快速開發、部署和擴充。

代理程式與 **MES/DP** 之間的通訊

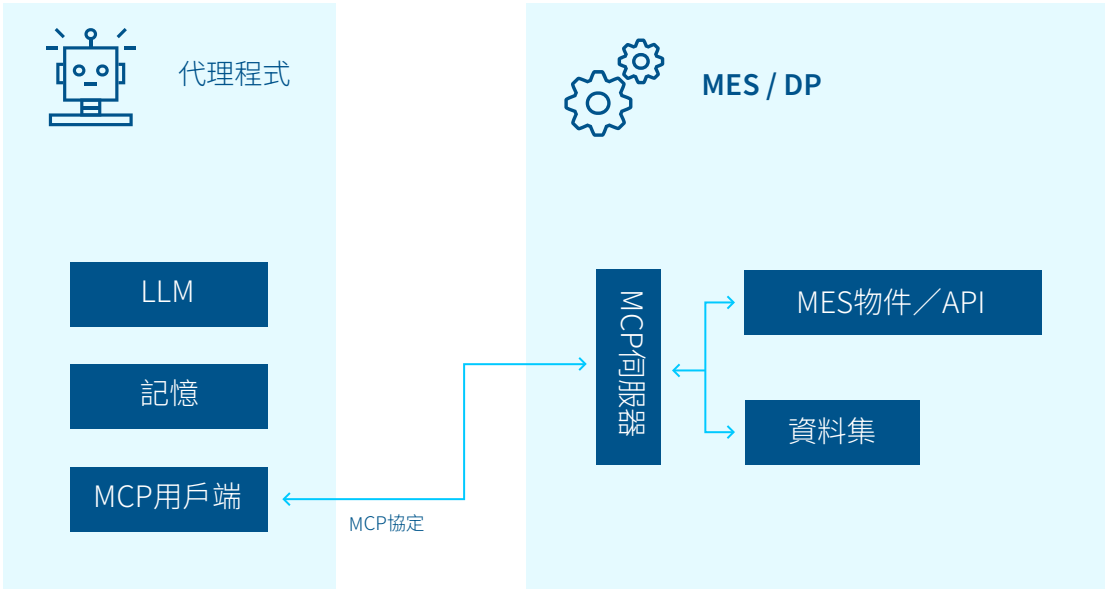

圖10:代理程式與MES/DP之間的通訊

代理程式間通訊 (A2A):智慧如何規模化

在複雜的製造環境中,沒有任何單一代理程式能完成所有任務。必須分散智慧。代理程式間通訊 (A2A) 使這成為可能。

透過A2A,專業化代理程式(例如排程、物料流或品質代理程式)可探索和協作。例如,如果物料流代理程式偵測到瓶頸,可通知排程代理程式。如果維護代理程式預料到故障,可通知品質代理程式以調整檢查頻率。

透過以MCP為基礎的結構化協定來進行這些互動。它們會被記錄、可觀測,並由共同政策治理。這讓工廠能夠進化成分散、協調並持續改進決策的智慧生態系統。

A24 - 代理程式間協定

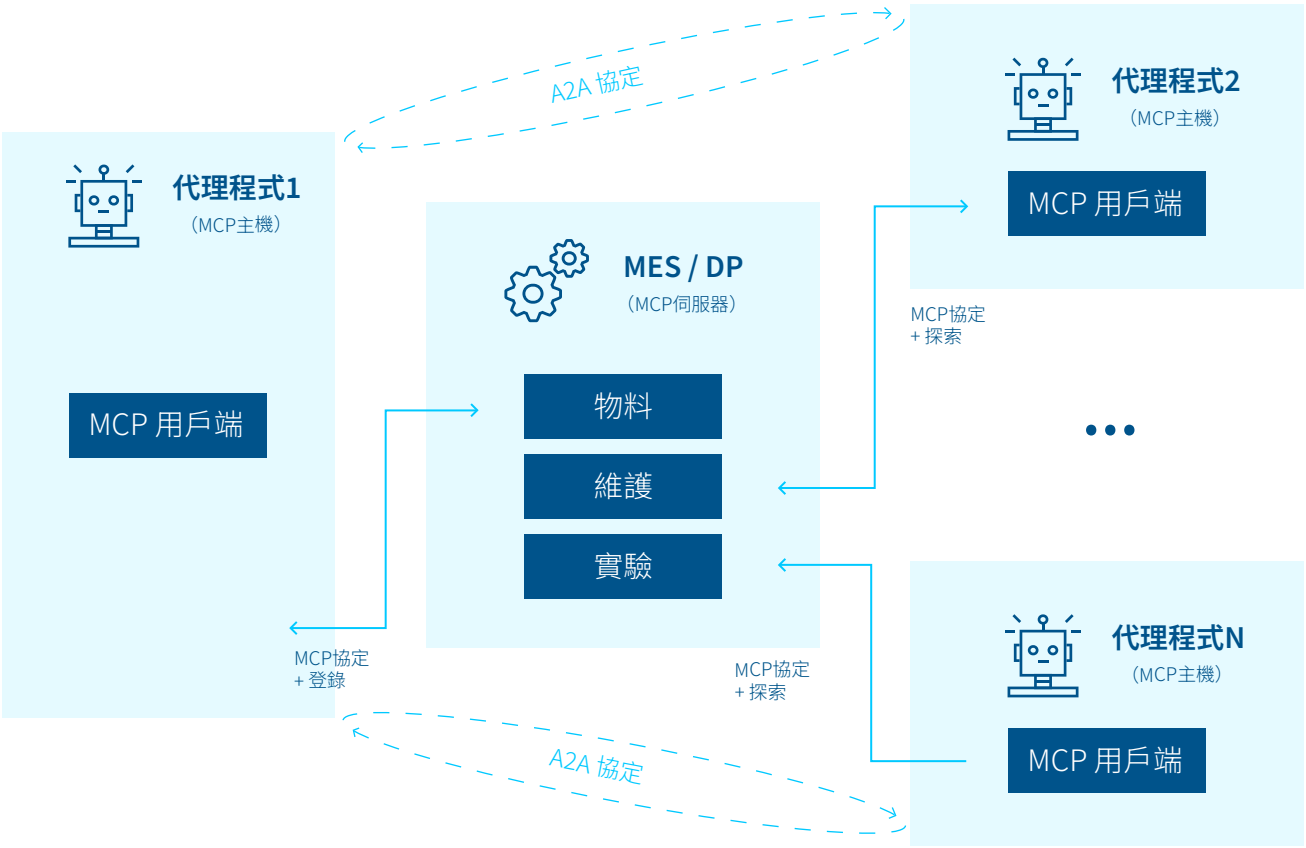

圖 11:A24 代理程式間協定

MES代理層級：從自動化到自主

MES向來都是由規則驅動。改用以代理程式為基礎的系統可導入各種智慧，或代理能力。

最低層級是靜態自動化：固定規則，無決策能力。代理工作流程提供更高的靈活性，在適應情境的同時仍在護欄內運作。自主代理程式則更進一步，利用推理、記憶和目標來做出決策，不需要預先定義的邏輯。在最高層級，協調代理程式監督並協調其他代理程式，以實現系統最佳化。

此演進可讓企業逐漸從確定性控制邁向自適應智慧，在每一步中獲得價值，同時維持作業安全和穩定性。

MES 代理層級

圖 10：MES 代理層級

MES AI代理程式的學習循環

AI代理程式的特色在於學習。它們執行行動、觀察結果，並根據成果來調整行為。這形成持續改進的循環。

例如，排程代理程式可重新安排工作以縮短週期時間。如果變更可提高產量，代理程式就會強化該行為。如果導致延遲，則會進行調整。人類回饋（例如核准、否決或操作員註解）會輸入至代理程式的記憶中，有助於精進未來決策。

此循環讓MES能夠動態演變，隨著時間而不斷改進，不需要手動改寫程式。系統不僅將任務自動化；執行任務的能力也越來越強。

MES AI代理程式的學習循環

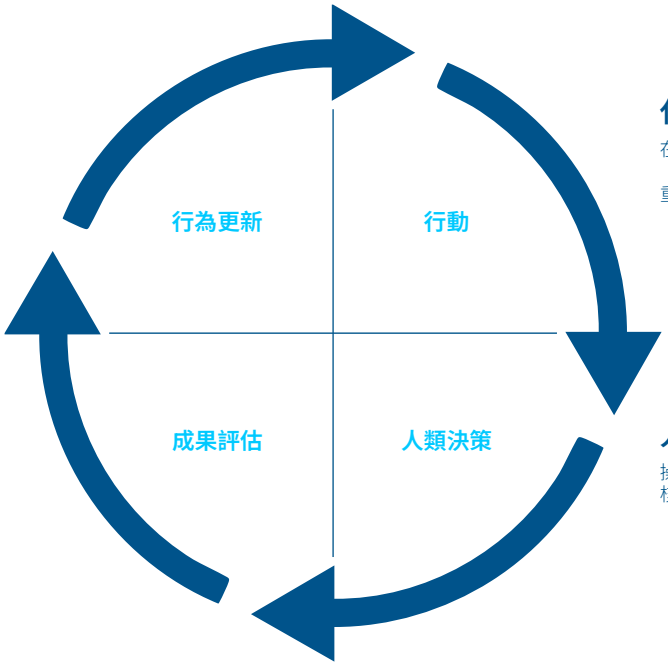

圖 13：MES AI代理程式的學習循環

製造業AI代理程式的安全機制

製造業自主得來不易。AI代理程式必須在嚴格的安全和治理約束下運作。

政策執行可確保代理程式留在預先定義的界限內，例如絕不繞過安全檢查或修改已驗證的程序。人類參與監督可讓操作員核准或否決代理程式決策，尤其是在關鍵情境下。由於決策透明化，代理程式的每個行動都可追溯：使用哪些資料、為何採取行動，以及預期達成的目標。

這些機制讓AI代理程式自主行動，同時保持問責並符合營運目標和法規要求。

AI代理程式安全機制

圖 14：AI代理程式安全機制

給製造業高階主管的策略性重點

改用以代理程式為基礎的MES並非可能性的問題，而是準備程度的問題。成功需要對資料架構、整合和治理進行基礎投資。

高階主管必須先整合自動化、MES和資料平台，以共同的語意模型為中心。接著，在可控且高價值的應用情境中試行代理工作流程。盡早建立回饋循環，尤其是涉及操作員和管理者的回饋循環，並從一開始就導入安全控制措施。

這不是IT升級，而是營運模式轉變，從控制到協作，從配置到認知。及早行動者將引領下一個工業智慧時代。從傳統MES轉移到以代理程式為基礎的智慧系統不僅是技術演進，更是新的製造典範的開始。隨著AI代理程式變得更強大、更緊密連結並且更深入運作邏輯中，工廠將不再需要僵化的由上而下指揮。系統本身將開始展現智慧。

這些代理程式可預測故障，跨多個目標將效能最佳化，並從每個班次中學習。它們不會取代人類，但會改變人類必須關注的重點。營運將從介入轉為監督，從反應轉為改進。

這就是思考型工廠：不僅運作，還能推理的系統。此系統能夠適應，也能改進，並且充分發揮AI的潛力，讓它不只是工具，而是製造業本身的原生功能。

從業務規則到代理程式：**MES** 堆疊的演進

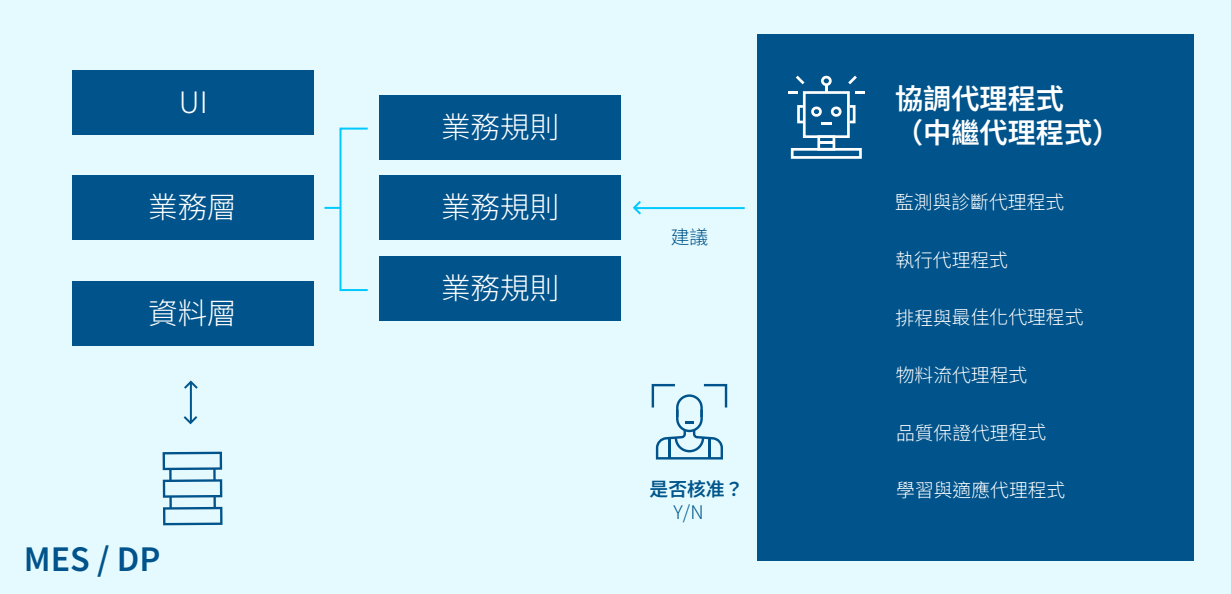

圖15：從業務規則到代理程式：MES堆疊的演進

關於作者

Francisco Almada Lobo被公認為數位轉型領域的頂尖策略思維領導者兼傳播者，尤其是工業4.0、製造營運和未來工廠。Francisco於2009年與其他人共同創辦 Critical Manufacturing，並自2010年起擔任CEO。

Francisco在CIM研發機構開始職業生涯，並於1997年加入Siemens Semiconductor。在Siemens、Infineon和Qimonda任職期間，他專門將高度複雜的離散製造業務最佳化。2004年，他在一家正在全速運作的大型工廠裡，完成了第一次 MES 系統的轉換。

Francisco在智慧製造和創投產業中擔任各種職位，包括200M Fund的投資委員會成員、SEMI智慧製造技術執行委員會成員、Forbes技術委員會成員以及多家工業4.0新創公司的顧問。

關於 CRITICAL MANUFACTURING

Critical Manufacturing提供最現代化、最靈活且可配置的製造執行系統 (MES)。Critical Manufacturing MES協助製造商滿足嚴格的產品可追溯性及合規性要求；以固有的封閉迴圈品質降低風險，與企業系統和工廠自動化完美整合，並提供全球生產營運的深度情報和可見性。因此，客戶為工業4.0做好準備。他們可以隨時隨地輕鬆調整營運以因應需求、機會或要求的變化，進而有效競爭並獲利。

欲深入瞭解，請造訪：www.criticalmanufacturing.com