

AI 如何改變物流與資產追蹤

編輯部整理

引言：從獲取資料到消費資料

資產追蹤產業正在進入由邊緣 AI、雲端 AI 與物理 AI 共同驅動的新階段。真正的技術價值不僅在於獲取資料，更在於如何利用資料做出決策。

AI 技術的融合與實際應用

AI 在資產追蹤領域的應用，不是簡單的增加一個對話介面，而是從邊緣到雲端，再到對物理世界的理解，完成了一套完整的架構演進。

邊緣 AI(Edge AI)：TinyML 與資料降採樣

在物聯網領域，一條基本的物理規律是：通過射頻天線發送 1 比特資料的能耗，通常是在本地微控制器 (MCU) 內執行上千次運算能耗的數百倍。這一規律在 2026 年推動了 Edge AI (尤其是 TinyML) 在資產追蹤終端的廣泛應用。

傳統的追蹤器是簡單的資料搬運工。例如，一台監控精密儀器的防震追蹤器，其內置的 6 軸加速度計會以每秒數百

次的頻率持續採集震動資料。如果將這些原始資料全部通過 5G RedCap 或衛星傳回雲端，不僅需要消耗大量頻寬，設備電池也會在短時間內耗盡。

TinyML 的端側自主決策：

2026 年，以意法半導體 (STMicroelectronics) 的 STM32N6 系列 (內嵌神經處理單元 NPU) 以及 Nordic 低功耗 SoC 為代表的邊緣算力晶片，將精簡的機器學習模型 (TinyML，模型大小通常只有幾十到幾百 KB) 直接部署到追蹤器的本地記憶體中。

— 智慧資料降採樣 (Smart Data Downsampling)：設備在本

地以 200Hz 的頻率採集原始波形，但不上傳原始資料。本地的 TinyML 演算法利用羽量級神經網路 (如一維卷積神經網路 1D-CNN 或隨機森林) 即時提取波形特徵，判斷當前的震動是正常的卡車引擎怠速抖動，還是異常的叉車裝卸摔落。

— 從傳資料到傳結果：當判定為正常震動時，設備靜默記錄；一旦識別出特定的“破壞性衝擊事件”，設備才喚醒射頻模組，向雲端發送一條精簡的語義結論 (例如：“警告：在座標 X/Y 處發生 8.5G 的垂直跌落事件，置信度 99%”)，並附帶跌落瞬間

圖說：AutoTrak 公司使用 STM32N6 建立的貨車司機行為追蹤系統



前後的 2 秒關鍵波形切片。

權威機構的報告顯示，採用 TinyML 端側異常識別技術後，新一代工業級追蹤器在保持異常事件捕獲率的前提下，無效資料上報流量減少了 85% 至 92%，設備續航時間顯著延長。Edge Impulse 的 CEO 在近期的訪談中表示："2026 年最好的物聯網傳輸協議，就是減少傳輸。在無網或弱網環境下，賦予邊緣節點自主決策能力，是實現永續供應鏈追蹤的有效途徑。"

雲端 AI(Cloud AI)：ETA 預測與全鏈路優化

如果說邊緣 AI 的任務是 "資料過濾與局部感知"，那麼雲端 AI 的核心使命則是 "全域時空挖掘與時效預測"。在全球供應鏈中，承運人與貨主最關心的指標是預計到達時間 (ETA, Estimated Time of Arrival)。

過去，ETA 的計算較為粗放，往往基於固定的航線時刻表加上簡單的距離除以速度。然而，真實的物理世界充滿變數：蘇伊士運河通行受阻、巴拿馬運河乾旱限行、港口工人罷工、暴風雪災害等，任何一個因素都會讓傳統的 ETA 失效，引發下游工廠停工。

2026 年基於大模型的 ETA 預測系統：

過去一年半，隨著雲端

算力基礎設施的發展，頭部供應鏈平臺 (如 Project44 聯合 Google Cloud 等) 將生成式 AI 與海量時空軌跡分析結合，推出了新一代 Predictive ETA (預測性到達時間) 系統。

這一系統將多維特徵流持續輸入雲端的時空圖神經網路 (Spatio-Temporal GNN)：

1. 資產硬數據：數百萬個集裝箱追蹤器傳回的即時座標、移動速率與滯留狀態。
2. 基建軟數據：全球各大港口碼頭作業系統 (TOS) 的即時擁堵指數、泊位排隊船舶數量、內陸鐵路轉運站的底盤車 (Chassis) 可用率。
3. 宏觀環境變數：全球高解析度氣象預測模型資料、即時洋流風向，以及結合 NLP (自然語言處理) 技術從全球新聞中抽取的 "地緣衝突與罷工情緒指數"。

通過這種全域特徵的融合計算，雲端 AI 能夠發現人類難以察覺的非線性關聯。

物理 AI (Physical AI)：數位孿生與智慧控制塔

2026 年科技界關注的概念之一是 "物理 AI (Physical AI)" (由 NVIDIA 等算力巨頭在 2026 年初的行業大會上重點推廣)。物理 AI 強調 AI 模型必須理解和遵循真實物理世界的重力、空間拓撲、動力學以及時間連續性。在資產追蹤領域，物

理 AI 的落地形態是供應鏈數位孿生 (Supply Chain Digital Twin) 與智慧控制塔 (Control Tower)。

傳統的供應鏈控制塔大多是一個靜態的 BI (商業智慧) 儀錶盤，用紅綠燈顯示貨物狀態，且滯後於物理現實。而 2026 年的物理 AI 控制塔，是建立在千萬個邊緣追蹤節點即時資料基礎上的全景模擬與編排引擎。

系統在雲端 1:1 構建了一個三維數字世界。每一條行駛在大西洋上的貨輪、每一輛在公路上行駛的冷鏈卡車、每一個堆疊在倉庫深處的智慧託盤，都在雲端擁有同步移動、同步感知溫度與震動的數位分身。

基於物理 AI 的空間計算與物理模擬能力，這個數位孿生控制塔具備了 "假設性 (What-if) 沙盤推演" 功能。

當系統捕捉到某港口突然發生擁堵時，物理 AI 會在虛擬沙盤中生成數千條平行的應對策略進行演練。如果將這批集裝箱緊急在另一港口卸貨，然後通過鐵路轉運，沿途的氣溫是否會導致醫藥產品超溫？鐵路轉運的額外成本與延誤的違約罰金相比，哪種方案的總體財務量化資料更優？沙盤推演完畢後，控制塔輸出最優的物流路由重新規劃 (Rerouting) 指令，並自動派發給承運商系統。

得益於全程視覺化與精準預測，企業不再需要因為 "擔

心貨物丟失或晚到”而堆積高額的安全庫存 (Safety Stock)。當整個企業的物流調度、財務理賠甚至碳稅核算都依賴於這些 IoT 追蹤終端時，一個潛在風險暴露出來：如果注入雲端 AI 的底層資料從一開始就被篡改或偽造呢？

截至 2026 年 8 月，隨著歐盟《網路韌性法案》(CRA) 進入強制執法階段，資產追蹤行業開始重視零信任安全。同時，AI 在接管控制塔後，正從“僅提供建議”的預測階段，向能夠自主談判、自主改簽的 Agentic AI (代理人工智慧) 方向發展。

網路安全與零信任硬體 (應對歐盟 CRA 法案)

物流資產追蹤的硬體設備常年暴露在不可控的環境中——它們可能散落在偏遠港口、公路驛站，甚至落入貨物盜竊團夥手中。這種物理暴露使得傳統的基於軟體密碼的網路防禦體系面臨挑戰。

在 2024 至 2025 年間，針對高價值供應鏈的“資料投毒 (Data Poisoning)”與“感測器欺騙 (Sensor Spoofing)”案件明顯增多。例如，跨國醫藥盜竊團夥利用軟體定義無線電 (SDR) 設備，對承載高價疫苗的冷鏈卡車實施 GPS 信號欺騙，讓雲端控制塔誤以為卡車仍在既定路線上行駛，而實際上車輛已被劫持。在另一些

案件中，不法承運商為了逃避冷鏈失溫導致的違約金，通過物理手段破解追蹤器，修改本地快閃記憶體中的溫度歷史記錄，以此騙取保險理賠或向貨主掩蓋藥品已失效的事實。

面對 IoT 終端安全問題，歐盟在 2024 年底通過了《網路韌性法案》(CRA, Cyber Resilience Act)，並在 2026 年初進入過渡執法期。CRA 法案規定，所有帶有數位元元素的硬體產品 (特別是直接接入網路的工業級 IoT 終端)，在進入歐洲市場前必須具備“默認安全 (Secure by Default)”與“設計安全 (Secure by Design)”的資質。如果因設備安全性漏洞導致資料洩露或供應鏈基礎設施癱瘓，設備製造商將面臨高達全球營業額 2.5% 或 1500 萬歐元的罰款。

歐洲網路與資訊安全局 (ENISA) 執行主任在 2026 年 3 月的布魯塞爾網路安全峰會上向全球硬體廠商表示：“在物理 AI 統治供應鏈的時代，資料就是決策本身。如果不能在硬體層面保證感測器資料的完整性與不可抵賴性，那麼雲端的大模型和數位元孿生，也只是建立在不可靠基礎上的虛像。”

為了跨越歐盟 CRA 的合規門檻並防範資料篡改，2025 年至 2026 年，全球資產追蹤硬體廠商開始從單純依賴軟體加密的架構，轉向引入獨

立硬體安全元件 (SE, Secure Element) 與物理不可克隆功能 (PUF, Physically Unclonable Function) 晶片。

以恩智浦 (NXP) 的 EdgeLock SE050 升級版以及英飛凌 (Infineon) 的 OPTIGA Trust M 系列為代表的安全晶片，已成為高端資產追蹤器的標配。這種硬體級零信任架構的運作邏輯如下：

首先，PUF 技術利用半導體製造過程中的微觀物理差異，為每一台追蹤器生成一個獨一無二、且無法被讀取或複製出矽片外部的底層私密金鑰。即便是追蹤器的製造廠商或雲平臺管理員，也無法知道這個私密金鑰。

其次，當設備邊緣端的感

圖說：NXP EdgeLock SE050 晶片



資料來源：NXP

圖說：Infineon OPTIGA Trust M 晶片



資料來源：Infineon

測器 (如溫度計、IMU 震動感測器、GNSS 模組) 採集到資料後, 資料流程會直接送入獨立的 SE 安全晶片中。SE 晶片利用 PUF 生成的底層私密金鑰, 在晶片內部的隔離 "安全飛地 (Secure Enclave)" 中, 對每一條溫度記錄和座標打上不可篡改的加密數位簽章 (Digital Signature), 然後再通過蜂窩網路發送至雲端。

在這個閉環中, 任何試圖在外部匯流排上截獲並修改溫度資料的行為, 或者試圖用模擬器偽造 GPS 座標的欺騙攻擊, 都會因為無法生成匹配的數位簽章而在雲端驗證時被識別。通過這種 "硬體加密上鏈" 的機制, 企業不僅符合了歐盟 CRA 的要求, 更確保了給物理 AI 進行沙盤推演的資料是真實、可信且具有法律審計效力的。

預測性韌性 (Predictive Resilience)

2025-2026 年的地緣政治

變化中, 海峽封鎖、港口罷工以及極端氣候帶來的斷航事件頻發。物流業界意識到僅僅做到 "全域可視" 是不夠的, 必須走向 "預測性韌性 (Predictive Resilience)"。

傳統供應鏈的回應機制是一種 "事後補救 (Reactive)" 模型。當貨輪被堵在蘇伊士運河外, 或者集裝箱已在中轉港口被錯誤堆放三天, 控制塔才會亮起紅燈。此時, 交期延誤已成為事實, 供應鏈經理只能向客戶道歉、支付違約金, 並花費高額運費緊急包機補發貨物。

在 2026 年由多模態 AI 驅動的 "預測性韌性" 模型下, 這種情況被提前阻斷。得益於 "千萬級無源 IoT 節點" 與 "低軌衛星全天候推流" 技術, 雲端圖神經網路 (GNN) 如今擁有了細顆細微性的即時物理坐標系。當這些軌跡資料與全球海關政策變動、港口氣象雷達以及新聞情緒監控 (NLP) 模型結合時, AI 便具備了 "事前規避

" 能力。

Agentic AI 與零碳無源 IoT

在未來三年內, 兩大趨勢將改變行業的操作方式。

在當前的預測性控制塔中, AI 的角色是 "顧問" —— 它負責收集資料、發現危機、計算方案並給出建議, 但最終在系統中點擊確認、發送改道郵件、向承運商談判運費動作的, 依然是人類調度員。

然而, 自 2026 年年中開始, 隨著大模型推理能力的提升, 行業正向 Agentic AI (自主代理人工智慧) 方向發展。

在 Agentic 時代, AI 不僅擁有 "眼睛" 和 "大腦", 更被賦予直接作業系統與商業談判的 "手腳"。當未來的智慧醫藥冷藏箱探測到乾冰即將耗盡時, 它將不再只是向雲端報警。嵌入控制塔的 Agentic AI 將作為一個獨立的數位元代理, 自主運行一套複雜的邏輯流:

它會自主登錄航空公司的

表：2026 供應鏈追蹤終端安全架構演進對比中：安全防禦

安全防禦維度	傳統軟體加密架構 (Pre-2025)	零信任硬體 SE/PUF 架構 (2026 歐盟 CRA 合規版)	防範價值
金鑰存儲機制	存儲於主控 MCU 的普通快閃記憶體中。易通過物理探針或固件提取被駭客攻破。	PUF 矽片指紋。金鑰在設備斷電時消失, 通電時利用物理特性即時重建, 實體層面上無法提取。	杜絕設備被惡意克隆, 防止駭客偽造假設備向雲端發起資料污染攻擊。
感測器資料防偽	僅在網路傳輸層 (TLS/SSL) 加密。本地資料產生到發送前仍為明文, 可被攔截篡改。	端到端硬體數位簽章。溫度與座標在生成的微秒內即被 SE 晶片打上專屬防偽印記。	防止 "篡改溫度逃避理賠" 的行為, 確保醫藥冷鏈溯源檔案具備法律效力。
OTA 固件升級	驗證機制較弱, 易被植入惡意木馬, 淪為發起 DDoS 攻擊的跳板。	基於信任根的硬體安全啟動 (Secure Boot)。非官方簽名的任何底層代碼將被物理拒絕執行。	滿足 CRA 法案對設備生命週期內安全補丁更新的監管要求。

貨運 API 介面，比對當天所有可用的艙位；它能通過自然語言或 EDI 與機場的地勤系統進行「機對機 (M2M)」交互，自主下單並支付費用，雇傭一輛冷鏈轉運車前往停機坪進行搶救；它甚至可以根據最新的電子合同條款，自動生成理賠報告併發送給保險公司的自動化定損系統。

NVIDIA 創始人黃仁勳 (Jensen Huang) 在近期的產業對話中指出："Agentic Workflow (代理工作流) 將是工業數位化的重要方向。未來的供應鏈不再需要人類坐在螢幕前去點擊按鈕應對異常。海量的智慧硬體將與自主 AI 代理對話，它們會在人類休息的時候，修復那些即將斷裂的物流鏈條。"

零碳無源 IoT 與碳交易體系

隨著技術與商業模式的成熟，合規性將在 2026 年之後成為主導硬體架構的重要推手。正如前文分析的，歐盟的 DPP (數位化產品護照) 只是一個開始。

隨著全球碳邊境稅 (CBAM) 與 Scope 3 (價值鏈上下游間接排放) 審計常態化，2026 年之後，任何帶有電池且生命週期結束後面臨回收成本的傳統追蹤器，都將面臨市場壓力。

以 5G-A 環境射頻能量收集和微光能 PMIC 為核心的「零碳無源 IoT」，將與全球碳交易與綠色金融體系進行綁定。未來的每一個木託盤、每一個共用周轉箱，其內置的無源標籤不僅僅是在上報軌跡，更

是在即時生成經過零信任晶片加密的綠色數位資產。企業不僅能通過精確的里程換算免除環境稅，甚至可以通過向碳交易市場出售經過驗證的減排額度，將資產追蹤從「合規工具」轉化為「綠色收益來源」。

結語：物理世界的數位元化

「萬物互聯」這一概念，正在與物流與資產追蹤產業結合。從被動的靜態記錄，到中途的動態介入，再到未來自主協商的 Agentic AI。物流與資產追蹤產業已跨越了僅僅回答「貨物在哪裡」的階段。它正在將數以億計的集裝箱、託盤與卡車，編織成一個具備感知、修正與思考能力的有機網路。

CTA

國海院發布 MDImageNet 高品質海廢資料集啟動海廢辨識國際 AI 競賽

為提升海洋垃圾監測效率並加速海洋治理數位轉型，海洋委員會國家海洋研究院 (下稱國海院) 近日發布全臺首套 AI-Ready「MDImageNet 海廢影像資料集」，同步啟動「2026 海廢影像辨識國際 AI 競賽」。本次活動由海洋委員會指導，Amazon Web Services (AWS) 提供 AI 技術支持與雲端服務資源，工業技術研究院 Aldea 人工智慧共創平臺負責競賽執行，透過資料集開放與國際競賽雙軌推動，攜手產官學研共同發展海洋垃圾智慧辨識技術，打造海洋治理數位公共基礎。

國海院表示，海洋垃圾會隨海流跨境漂移，臺灣海岸同時承受在地與境外海廢累積，傳統海岸調查須仰賴大量人力進行撿拾、分類、量測、拍照及登錄，後續仍需耗費時間整理照片、核對資料與統計分析，效率有限且不易維持一致的判讀標準。為提升監測效率，國海院歷時多年建置 MDImageNet 海廢影像資料集，目前已累積超過 2 萬張真實海岸影像，完成逾 4.2 萬個海廢物件標註，建立符合 AI 模型訓練需求的高品質資料集。資料集以國際淨灘行動 (ICC) 分類為基礎，進一步建立 NAMR 三層級分類架構，兼顧國際接軌與國內調查需求，並依循《人工智慧基本法》推動資料治理、資料開放、共享及再利用方向，以 CC BY 4.0 授權釋出，提供研究機構、教育單位及產業界共同投入海洋 AI 創新應用。

國海院指出，透過公私協力與國際社群參與，逐步建立從資料、模型到治理應用的海洋科技生態系，讓 AI 成為提升海洋調查效率、支援科學決策及守護海洋環境的重要力量。