INSTITUTE FOR
INFORMATION
INDUSTRY

軟體技術篇

數位服務

產業躍升
為臺灣數位產業奠基公共智慧服務基盤

智慧軟體

守護車輛軟體安全
未來移動安全信賴評測中心掛牌上路

iii EVOLUTION
資策會45週年

軟體技術研究院

產業躍升
為臺灣數位產業奠基
公共智慧服務基盤

為協助資服業者快速打造公共智慧服務應用，資策會規劃與建置所需的公共智慧服務基盤（Public Intelligent Service Architecture, PISA），可吸引資服業者，以公私協力方式，參與智慧公共服務的打造，發展有感的數位公共智慧服務。

可信任
- 必須讓民眾信賴的系統
- 驗證身分、可靠的各種服務、保護使用者數據的隱私和安全
- 確保內容與資訊正確

互通性（Interoperable）
- 開放的標準、程式碼和數據存取
- 印度的通用支付介面UPI（支付服務單一介面，無縫接軌和帳戶對帳戶的互通性）

公共性
- 確保使用情境讓人民受益
- 非營利組織哈克達薩克（Haqdarshaq）的「輔助技術」模式，賦能社福人員
- 愛沙尼亞的 X-Road 平台允許各個政府機構、企業和公民之間進行安全的資料交換

韌性（Resilience）
- 能應對快速變化的危機
- 烏克蘭的Diia（數位文件共享、身分識別、130種政府服務入口、戰前用於Covid疫苗接種證明，戰爭爆發後迅速重新部署，變成能夠給付公民現金、並為戰火中失學的孩子提供數學教室）

永續經營
- 健全的生態系統，商業模式確保有足夠自償率並自給自足的永續經營
- 開源健康數據管理平台DHIS2，100個國家，涵蓋23億人生態系統

公共智慧服務應用（PISA）的特性

隨著數位化的迅速進展，數位公共智慧服務系統，在數位轉型、治理和數位生態方面顯得至關重要，尤其在OpenAI的ChatGPT發表後，引爆一股生成式AI熱潮，資服業者前仆後繼嘗試投入AI模型訓練，政府需要制定整體數位公共智慧服務推動戰略和數位治理政策。

訓練資料、AI模型以及大量算力為AI必備三元素

AI的模型訓練往往需要訓練資料、AI模型以及大量算力，已成為發展AI應用服務發展的痛點與投資成本，這三者都是資服業者最迫切需要的協助。

過去新創團隊想開發AI服務，只能單打獨鬥，開發過程所需的訓練資料、AI模型、應用程式及開發框架，一切都得自己來。臺灣資服業者在面對複雜的AI模型訓練時，受限於資源，只能選擇通用型的大型語言模型短期練兵。通用型的模型無法一體適用，還需再客製化修正，導入更細緻的專業領域知識（Domain Know-How），才能切合需求。

AI模型訓練的另一個門檻是算力。AI模型訓練是嘗試錯誤（trial and error）的過程，透過反覆訓練提高AI人工智慧的精準度，逐步做到品質的收斂。有好的產品或服務，才有機會落地，創造優質的商模。這些過程都需消耗大量的算力及資源，而算力要價不菲，有的團隊買不到足夠的算力，有的團隊則是拿不到好的訓練資料，種種的阻礙，造成許多新創團隊雖有雄心大志，卻往往做到一半，計畫就胎死腹中。

公共智慧服務基盤（PISA）加速發展，開發省時省力

為解決資服業者的痛點，並降低資服業者開發AI應用的重複投資，公共智慧服務基盤（PISA）匯聚資服業者所需要的重要AI基礎元素，方便業者更快的開發和部署AI應用程序，也更容易進行資源共享。

如同政府興建工業區，要先興建廠房，拉好水電，鋪設聯外道路及設置路燈，公共智慧服務基盤（PISA）則是把資服業者所需要的訓練資料、算力及AI模型整備齊全，讓企業站在穩固的基礎上進行開發，快速形成服務，跨過AI訓練的門檻。

比如，某家資服業者想要打造一套金融創新服務，但是缺少金融領域的專業數據，透過公共智慧服務基盤（PISA），企業可依據預算及需求，直接採用想要的訓練資料、模型及開源AI演算法，再導入銀行端的專業領域知識，就可進行開發。平台還會根據需求，提示相關的數據曾用在哪些開發項目，並推薦相關的開源程式碼，供新創團隊參考。

公共智慧服務基盤架構

公共智慧服務基盤（PISA）提供的訓練資料與程式碼都經過隱私強化與資安驗證，等於業者可在一定品質的既有基礎上，快速發展服務，無須擔心底層的基礎設施，並可專注打造滿足需求的解決方案。如此可避免無謂的重覆開發，降低開發成本。根據過去經驗，3個月的AI開發時程，透過公共智慧服務基盤（PISA）的支援，可大幅縮短到1.5個月，企業可節省開發時間達50%以上。

開源共享，公共智慧服務落地

基於普惠共享理念，公共智慧服務基盤（PISA）中的訓練資料，鏈結政府與企業的訓練資料，符合規範、互信的相互交換，以區塊鏈技術存證，串接第三方線上計費及金流服務。

以往大語言模型 Llama2 7B的訓練微調，業者使用雲端GPU得跑7天，使用公共智慧服務基盤（PISA）的算力，只要半天不到，就可以完成；並提供戰情室觀測整體系統，讓用戶了解使用狀態。

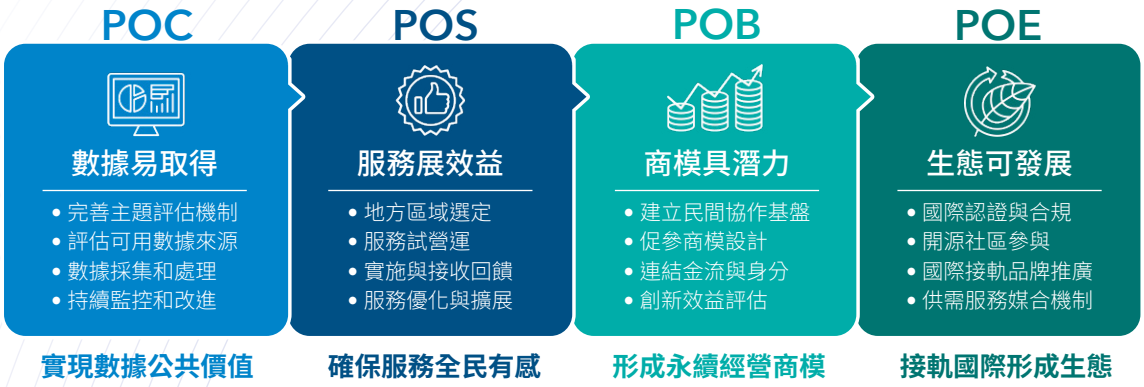
AI模型程式碼則提供資安檢核服務與弱點掃描及SBOM（Software Bill of Materials）分析，俾利業者在安全的共享基礎上進行驗證開發，也可將成果提供下載授權，供其他資服業者使用。

透過上述公共智慧服務基盤（PISA）設施，業者可依據多種應用情境，打造政府的數位公共智慧服務應用與企業的AI應用服務解決方案，強化軟體的公共建設，如社福機構的核銷流程繁瑣，必須符合不同的檔案格式與各種流程規定，工作人員為完成核銷，滿桌單據令人頭昏眼花，人工核銷又容易出錯，工作效率低落，人力負擔成本也很吃重。若能串接不同單位的訓練資料庫，透過公共智慧服務基盤（PISA），建立統一檔案交換格式，工作人員只需輕鬆上傳單據，後台使用AI模型辨識，便能快速進行核銷作業，大幅簡化核銷流程。又如照顧機構的人力不足，加上許多文件必須填寫，對於照顧機構員工是沉重的負擔，透過公共智慧服務基盤（PISA），發展照顧服務的智慧照顧文件生成代理人（AIAgent），協助自動生成行政文件，將減輕照顧機構員工的工作量，多一些時間照顧長者的需求。

公私協力共創，促進數位公共智慧服務應用

公共智慧服務基盤（PISA）將是臺灣數位產業發展及數位轉型的重要基礎建設，以生態系發展的方式，引導公私協力創新，催生典範的公共智慧服務，期盼建構良好的AI產業發展環境。有了公共智慧服務基盤（PISA）為基礎，資服業者可放心在信賴的平台上設計解決方案，為消費者打造更好的產品與服務。

未來，公共智慧服務基盤（PISA），業者可藉此產生良善的數位生態系。公共智慧服務基盤（PISA）也可進行典範轉移，擴及到其他數位公共建設，促進公共服務共創，推進基建領域的建設，為臺灣打造優質的數位產業生態系，提升數位國力。



公共智慧服務基盤典範轉移至生態擴大

軟體技術研究院

守護車輛軟體安全
未來移動安全信賴評測中心掛牌上路

電動車、自駕車與車聯網等嶄新技術使得未來移動的生活面貌有了極大的突破，車輛市場在硬體評測方面早已有健全的審核機制，但在車載系統的評測方法、工具及制度方面，臺灣仍在起步。資策會新揭幕的「未來移動安全信賴評測中心」首度提供AI感知、通訊韌性及資安防護三種評測項目，結合具多元混合天候人車流的「Formosa臺灣街景深度學習資料庫」，為智慧車輛產業打造穩固的護城河，企盼以研發成果推動智慧車輛產業的升級，擘劃安全的未來移動跨域生態藍圖。

為減少人為的操作失誤，而有了自駕車（Autonomous Vehicles, AV）的問世。隨著先進駕駛輔助系統（Advanced Driver Assistance Systems, ADAS）的普及，加上AI技術的突飛猛進，人們雀躍著或許可以解放雙手；但在邁向未來移動的路上，似乎還是有一點顛簸。

在舊金山一場音樂節上，因湧入太多人潮，一度造成附近多輛無人計程車在馬路上打結；加拿大一名駕駛開上高速公路，把車輛交給自動駕駛系統，隨後放下座椅呼呼大睡。警察發現後進行取締，這輛車不但沒有減速，還以時速150公里的高速逃逸…。

現行車用軟體安全於AI感知、韌性通訊、資訊安全有其挑戰課題

目前的市場上，智慧車載系統已是新車的標準配備，依靠聯網技術與AI運算，車主可藉由語音助理觀賞數位串流影片、打電話；座駕配備的影像與雷達感測設備，則能做到盲點偵測、汽車防撞、自動煞停與跟車，保障行車的安全。不過無人自駕車上路以來，因軟體系統設計不良、網路頻寬壅塞等原因，還是造成不少事故，為確保未來移動載具的軟體功能安全可靠，2024年7月，資策會「未來移動安全信賴評測中心」正式掛牌上路，以第三方評測中心的角色，提供車輛AI、資安、通訊等評測服務，為業界補足車輛軟體評測的缺口，也為全臺車輛的軟體安全性把關。

座駕導入了AI系統，但你信得過嗎？

拜新興科技之賜，智慧車電的相關應用蓬勃發展，各大車廠近年都在致力於開發ADAS並導入AI感知設備，讓車輛的技術越來越先進，並在開發設計的環節中，把安全性與資安防護納入考量，盼能滿足駕駛對行車安全的要求。

隨著汽車大廠陸續把AI晶片部署到車載系統中，車載娛樂、環境感測、駕駛偵測、ADAS等都改由AI軟體搭配感測設備來主導，當車輛越來越依賴複雜的軟體系統來實現感知、決策與控制功能時，汽車製造廠也不禁擔憂起配備的AI系統是否安全可靠。

AI在車輛移動間要負責辨識目標，若演算法不正確，容易發生誤判並造成災難性的後果。國外就曾發生老人過馬路時，AI猶豫不決，最後把老人誤判成物品，釀成憾事。但現行的法規尚未涵蓋到AI準確度的相關規範，每次國際大廠詢問一階系統整合廠（Tier 1）及二階模組系統廠（Tier 2）：「你的AI系統到底準不準？」，供應商因缺乏第三方公正的評測報告，很難證明產品的水準。

資安與通訊韌性，誰來把關？！

資安與韌性也是智慧車輛的重要環節，電影《斷訊》中演出城市遭到大規模網路駭客攻擊，導致馬路上的智慧車輛連環追撞，這樣的科幻情節並不是不可能發生。車聯網的移動載具通訊設備在5G高速環境下可相互串連，連結到其他車輛、道路系統，把蒐集來的大量資料上傳到雲端，再經AI進行演算、決策與控制，若AI模型被資料竄改或是系統弱點遭到駭客入侵，就有可能上演遠端奪車、從他處控制煞停，讓AI誤判交通號誌等恐怖的情節。

資策會「未來移動安全信賴評測中心」即是針對未來自駕系統的感知定位、路徑規劃、車路協同等智慧駕駛情境，提供AI模型辨識精準度、車聯網韌性程度及車電模組資訊安全等三項評測，車輛供應商可將軟體送進中心進行評測，藉由會內常年累積的車電AI感知技術開發研究成果、雲端數據開發工具，及「Formosa臺灣街景深度學習資料庫」，協助車電業者提升AI模型功能驗證的準確度，並快速通過評鑑，取得具公信力的驗證成果。

混合車流街景資料庫優化測試成果

針對車廠在銷售前的道路實車測試，資策會所研發的「Formosa臺灣街景深度學習資料庫」能發揮極大的優勢。國際車廠即使在國外已先通過國際車規的驗證，到臺灣後還是需要進行在地化的安全參數調校測試。臺灣的行車環境相當複雜，國外車輛的ADAS即使已在當地先經過AI模型訓練，恐怕還是無法應付臺灣特有的機車瀑布，與汽機車行人混合用路的複雜路況。

而資策會「Formosa臺灣街景深度學習資料庫」對臺灣獨特的多元混合人車流用路環境，進行廣泛的資料蒐集與深度學習，已累積全臺所有縣市10萬公里以上的真實感測資料；蒐集了不同天候光影、時段、車流、行人與交通號誌，並標記混合車流等物件，以AI感知評測有助於國際大廠快速評估其AI感知系統的不足之處與進一步開發調校，讓智駕系統能更快學習與適應臺灣複雜的行車情境。

第三方角色推動車電產業智慧升級

「Formosa臺灣街景深度學習資料庫」所蒐集的駕駛情境多重感測資料情境豐富且具真實度，等同實際行車情境。廠商可在評測中心利用該資料庫進行實車感知系統測試，所測結果等同實際道路測試。過去車廠從開發、整合到測試的每一個環節，付出了極高的成本，若改至評測中心的軟體環境中評測，在軟體開發階段便可為廠商節省下在感知系統開發整合約80%的硬體階段（Hardware in the Loop, HIL）與實車階段（Vehicle in the Loop, VIL）的測試成本，大幅減輕車廠及下游供應廠的開發測試成本。

放眼未來，各大車廠持續投入智慧車輛技術研發，根據經濟部統計，未來年產值預估可高達340億元以上。資策會身為第三方協力機構，長期致力於投入智慧車電的科技前瞻研究，並與其他產官學研及第三方驗證機構合作，期盼能打造臺灣的智慧車輛評測生態系，幫助車聯網產業智慧升級。

2024年資策會與第三方驗證機構簽訂備忘錄，聯手推動「車用軟體AI感知評測」與「車用國際標準合規驗證」服務，期盼運用第三方評測中心的尖端技術與評測能量，攜手夥伴一同強化臺灣車電產業的核心競爭力，協助業者快速打入國際市場，突破智慧車電的應用框架，站上智慧自動化駕駛的世界舞台。

資策會成立未來移動安全信賴評測中心舉辦啟動儀式；圖為貴賓合影，由左至右：資策會 楊仁達副執行長、中華智慧運輸協會 陳國章理事、台灣車聯網產業協會 吳盟分理事長、資策會 卓政宏執行長、台灣電動車產業聯盟 葉儀晧理事長、電電公會電動車委員會 游文光召集人、台灣先進車用技術發展協會 沈舉三秘書長、資策會 軟體院 蒙以亨院長。

財團法人資訊工業策進會
INSTITUTE FOR INFORMATION INDUSTRY

中文官網 Facebook DxBAR