

2026 未來科技獎 亮點創新技術發表與商機媒合會：人工智慧 × 半導體光電通訊

LLM 驅動之工業物聯網 輕量型 AI 入侵防禦系統

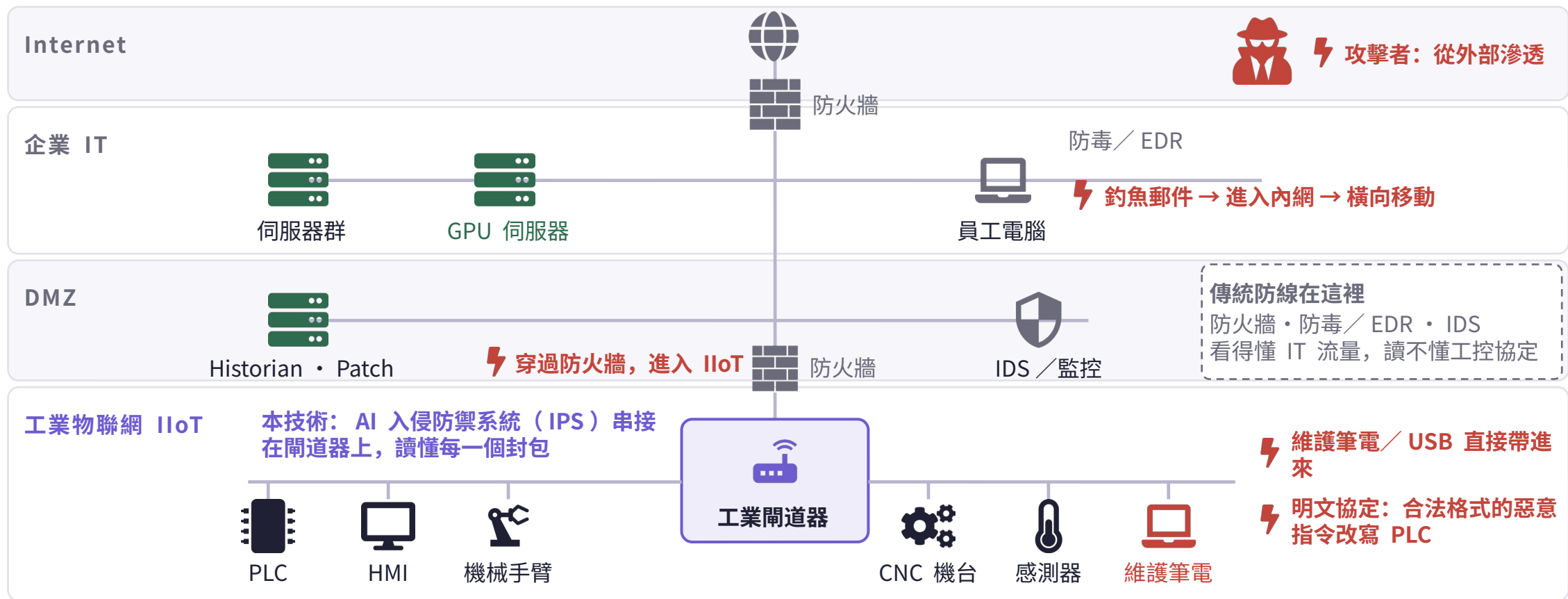
LLM-driven Lightweight AI Intrusion Prevention System for Industrial IoT

國立臺灣科技大學 資訊工程系 鄭欣明 教授 · 王紹睿 教授 · 蕭宗瑋 · 呂學易

國立陽明交通大學 資訊工程系 林盈達 教授

合作夥伴：威力工業 **ORing** · 智阜資安  CYBEROTLAB®

工業物聯網的網路架構與攻擊路徑



傳統防線守在門口，攻擊卻走得進來，攻擊一旦進到工業物聯網，只剩裡面能攔

IT 資安工具在工業物聯網的兩難

現場的兩難

- 開太鬆 — 格式合法的惡意指令直接改寫 PLC
- 開太緊 — 讀不懂工控協定，正常指令被擋，整線停機
- 一次非計畫停機，動輒數十分鐘到數小時
- 結果：多數業主選擇「只監看、不阻斷」

業主不怕沒有防護，怕的是「誤判停線」 — 設備買了，卻不敢開阻斷。

為什麼傳統方法做不到

1 特徵碼比對

只認得看過的攻擊，沒看過的完全漏掉

2 流量統計

看得到「量」不正常，看不懂「內容」在做什麼

3 工控協定本來就不一樣

Modbus、DNP3、S7comm 多為明文、無認證 — 一個格式完全合法的封包就能改寫 PLC

4 IT 資安產品照搬

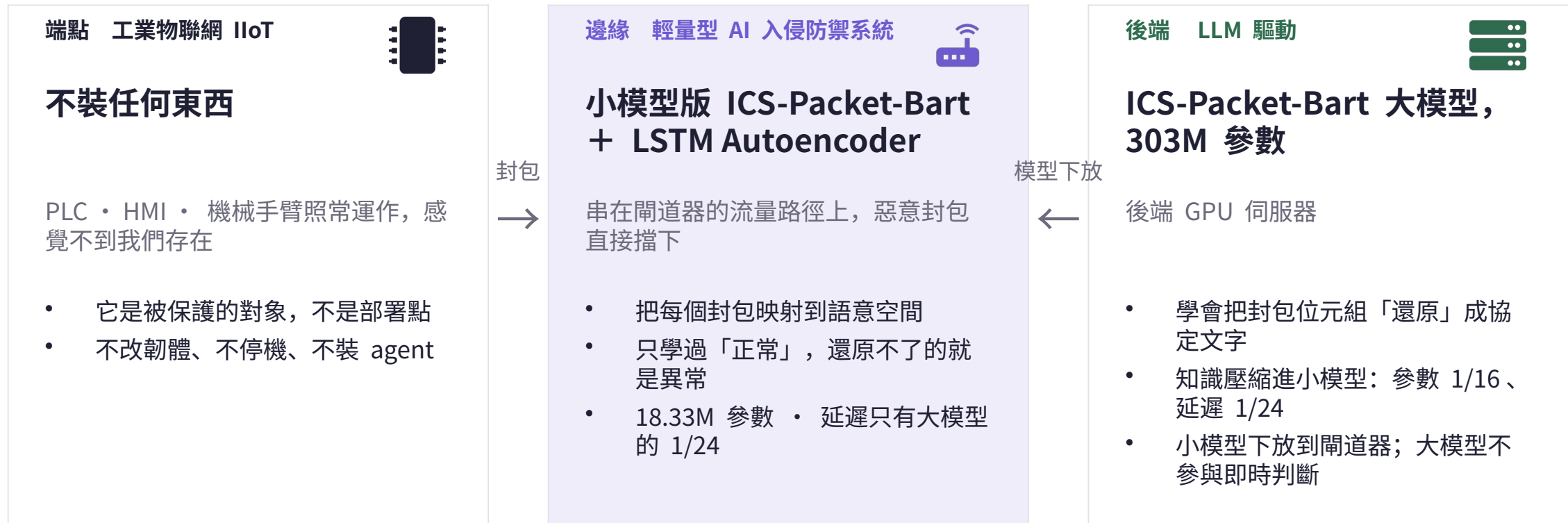
規則寫給 HTTP / HTTPS，讀不懂工控指令的語意，於是誤判

三層部署位置：端點、邊緣、後端



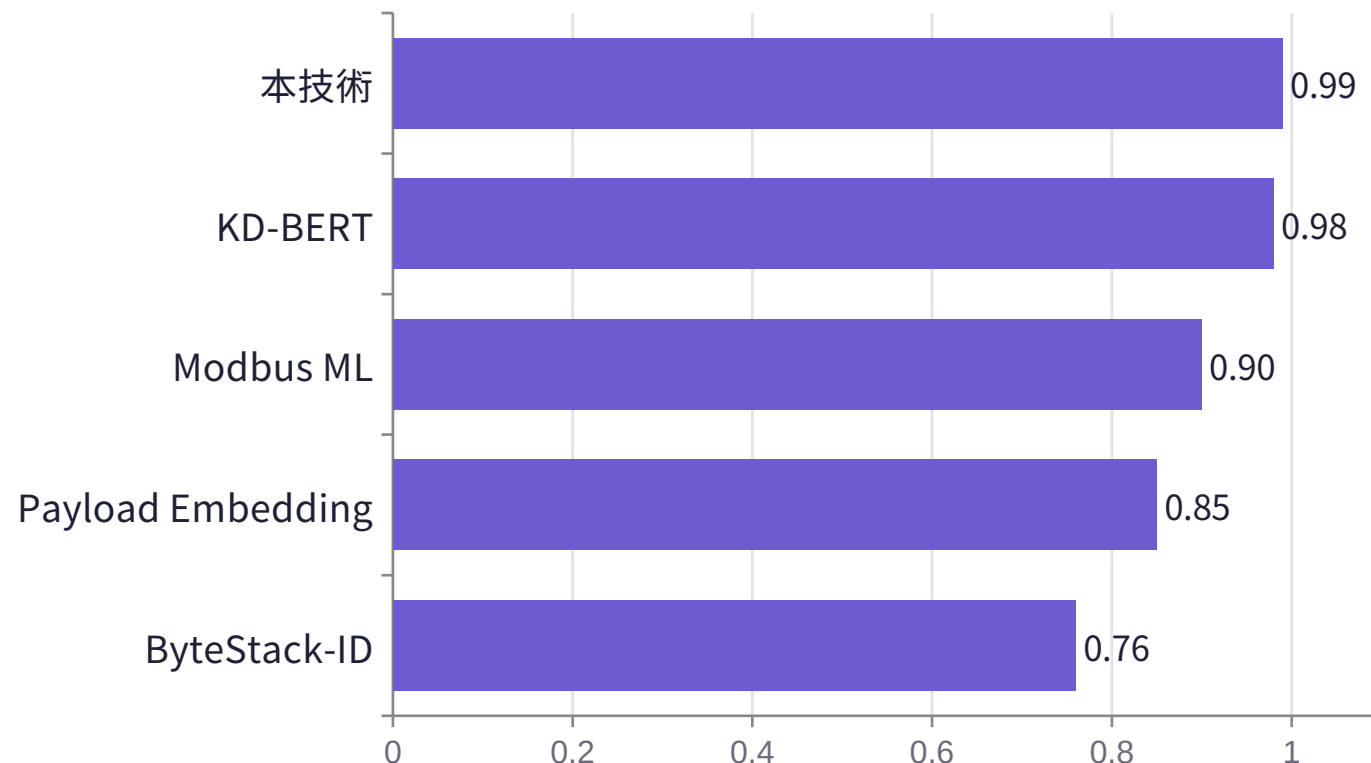
端點動不了、後端太遠 — 防護放在邊緣閘道器，換一台網通設備即可上線。

非對稱架構：後端 LLM 與邊緣輕量模型



LLM 在後端學會讀懂封包，輕量模型在邊緣即時攔截；已獲 IEEE Trans. Industrial Informatics 接受。

偵測效能比較



0.99

F1-score

攻擊發生 100 次，抓到 99 次；系統告警 100 次，99 次是真的。兩件事合起來打一個分數，滿分是 1.00。

抓得到，也不誤報

三組公開資料集、兩種工控協定（Modbus 與 DNP3）測試，F1-score 全數 0.97 以上。

未知攻擊的偵測原理

沒看過的攻擊，為什麼也抓得到？**因為模型從頭到尾沒有學過「攻擊」**

1 只用正常流量訓練

訓練資料裡一個攻擊樣本都沒有，也不需要攻擊標記

2 模型學會「還原」正常封包

把封包壓成語意特徵後，再還原回原本的指令內容

3 還原不了 → 就是異常

偏離正常語意的封包還原誤差會飆高，直接標記攔截

不是比對「像不像已知攻擊」，而是比對「像不像正常」——所以攻擊手法沒看過，一樣現形。

八類攻擊 — 進到工業物聯網後在線上做的事，訓練時全部沒出現過

重放正常指令	格式合法	99.94 %
偽造資料注入	格式合法	99.92 %
惡意載荷植入	格式合法	99.84 %
延遲回應	格式合法	99.80 %
全線圈寫入	格式合法	99.04 %
長度參數竄改	畸形訊框	99.86 %
查詢洪泛	流量型	99.88 %
低速位址掃描	偵察	94.58 %

封包格式完全合法，
特徵碼看不出來，
只有語意看得出來。

技術導入與應用場域

已導入設備

威力工業 **ORing**

- AI 內建於工業交換器／閘道器產品線
- 不需更動既有機台，換裝設備即可導入
- 邊緣即時推論，資料不離場域

可導入場域

半導體・能源・水處理・智慧建築・醫療

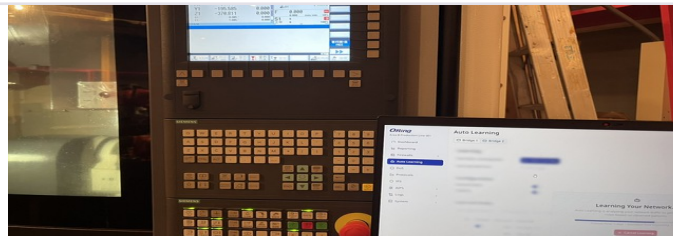
不再只是網路設備，而是「內建防護的網路設備」。

The screenshot displays the ORing AI IPS web interface. On the left is a navigation menu with options: Dashboard, Reporting, Firewalls, Auto Learning, DoS, Protocols, IPS (selected), AIPS, Logs, and System. The main content area is titled 'IPS' and shows configuration toggles for 'Intrusion Prevention System (IPS)' and 'Logging'. Below this is a 'Rules' section with a table of 7002 rules. The table columns are: Enabled, Rule ID, Category, Risk Level, Action, and Name. The rules list includes various CVEs such as CVE-2003-0719, CVE-2001-0537, CVE-2001-0892, CVE-2000-0234, CVE-2001-0241, CVE-2003-0352, CVE-2001-0241, and CVE-2004-0426. The interface also shows a sidebar for 'Area B Production Line 001' and a top bar with the date 'Jan 22, 2026, 12:25:13 PM'.

AI IPS 操作介面 — 規則、自動學習與即時阻斷



AI IPS 邊緣防護設備



CNC 機台現場導入

ICS Cracker：自動化紅隊引擎

起點 以攻驗防

光有防禦不夠，得證明它真的擋得住 — 所以我們自己寫了一支紅隊，反覆打自家的 AI 防禦。

- 拆解 Modbus、S7comm、OPC UA、MQTT、MAVLink、MELSEC 的攻擊手法
- 自動執行滲透、模糊測試、弱點掃描與阻斷攻擊，不停不累



ICS Cracker 檢測設備

ICS Cracker 操作介面

ICS Cracker 系統儀表板顯示了攻擊命令、ATT&CK 技術、CWE 弱點、OWASP 風險和 CERT 類別的統計數據。儀表板下方是一個表格，列出了各種漏洞和攻擊手法的詳細信息，包括漏洞 ID、名稱、嚴重性、影響和修復建議。

初始存取	執行	持久化	權限提升	防禦規避	探索	橫向移動	收集	命令與控制	抑制回應功能	損害流程控制	影響
T0860 Wireless Compromise	T0821 Modify Controller Tasking	T0857 System Firmware	T0874 Hooking	T0894 System Binary Proxy Execution	T0887 Wireless Sniffing	T0866 Exploitation of Remote Services	T0887 Wireless Sniffing	T0884 Connection Proxy	T0803 Block Command Message	T0836 Modify Parameter	T0829 Loss of View
T0819 Exploit Public Facing Application	T0807 Command-Line Interface	T0891 Hardcoded Credentials	T0890 Exploitation for Privilege Escalation	T0858 Change Operating Mode	T0888 Remote System Information Discovery	T0812 Default Credentials	T0850 Role Identification	T0869 Standard Application Layer Protocol	T0881 Service Stop	T0855 Unauthorized Command Message	T0831 Manipulation of Control
T0864 Transient Cyber Asset	T0863 User Execution	T0859 Valid Accounts		T0851 Rootkit	T0842 Network Sniffing	T0844 Program Organization Units	T0861 Point & Tag Identification	T0885 Commonly Used Port	T0800 Activate Firmware Update Mode	T0856 Spoof Reporting Message	T0837 Loss of Protection
T0810 Data Historian Compromise	T0858 Change Operating Mode	T0873 Project File Infection		T0872 Indicator Removal on Host	T0841 Network Service Scanning	T0843 Program Download	T0868 Detect Operating Mode		T0814 Denial of Service	T0806 Brute Force I/O	T0832 Manipulation of View
T0862 Supply Chain Compromise	T0853 Scripting	T0839 Module Firmware		T0856 Spoof Reporting Message	T0854 Serial Connection Enumeration	T0891 Hardcoded Credentials	T0801 Monitor Process State		T0805 Block Serial COM	T0875 Change Program State	T0815 Denial of View
T0865 Spearfishing Attachment	T0871 Execution through API	T0889 Modify Program		T0820 Exploitation for Evasion	T0808 Control Device Identification	T0859 Valid Accounts	T0845 Program Upload		T0816 Device Restart/Shutdown	T0833 Modify Control Logic	T0880 Loss of Safety
T0817 Drive-by Compromise	T0895 Autonomous Image			T0849 Masquerading	T0846 Remote System Discovery	T0886 Remote Services	T0811 Data from Information Repositories		T0878 Alarm Suppression	T0839 Module Firmware	T0828 Loss of Productivity and Revenue
T0866 Exploitation of Remote Services	T0875 Change Program State			T0824 I/O Module Discovery	T0867 Lateral Tool Transfer	T0802 Automated Collection			T0835 Manipulate I/O Image		T0879 Damage to Property

原本只是為了證明自家防禦擋得住 — 後來發現，工業物聯網設備製造商比我們更需要它。

合規檢測實績

已有實績 2026 / 06

協助威力工業閘道器通過 TÜV SÜD IEC 62443-4-2 SL2 認證，並取得歐盟 CRA 符合性聲明

- 認證機構不只看文件，還要看「這台設備有沒有真的被打過」— 弱點掃描與滲透測試的證據，最常卡關
- ICS Cracker 自動跑完、報告逐條對應標準，TÜV SÜD 直接採納為發證依據
- 工業物聯網設備製造商出貨前先在廠內跑一遍，不必等委外檢測（動輒百萬、排隊數月）才知道哪裡不過

歐盟 CRA

網路韌性法 • 2027/12 全面適用
威力工業已取得符合性聲明（VOC）

IEC 62443

工控系統資安標準
威力工業閘道器已通過 4-2 SL2

SEMI E187

半導體設備資安標準
ICS Cracker 內建條文逐項評估

衍生新創「智阜資安」（CyberOTLab，2025/10 成立）承接產品化 • 夥伴：工研院 • TÜV SÜD • TÜV 萊茵 • 資策會

合作邀請

1 製造與關鍵基礎設施 — 防護

在真實場域導入 AI 入侵防禦系統，共同定義需求

2 工業物聯網設備製造商 — 檢測

出貨前用 ICS Cracker 完成 CRA / IEC 62443 / SEMI E187 自檢，縮短認證時程

3 投資與通路夥伴

智阜資安尋求技術投資與國際通路，把台灣的工業物聯網資安帶進歐盟市場

Q & A

謝謝聆聽



智阜資安 CyberOT Lab

AI 防護 × 攻防模擬 × 合規證據

AI IPS 本技術的產品化 — 工控協定語意偵測、串接式即時阻斷

ICS Cracker MITRE ATT&CK for ICS 攻擊模擬、合規證據輸出

夥伴：ORing · 工研院 · TÜV SÜD · Fortinet · 臺科大 · 中山大學 · 資策會



cyberotlab.com



info@cyberotlab.com



smcheng@
mail.ntust.edu.tw



2026/06/17 · 新加坡 TÜV SÜD PSB 頒證

威力工業通過 IEC 62443-4-2 SL2 認證並符合歐盟 CRA，攜手智阜資安強化工業網路資安

經濟日報 2026/06/18 · 智阜資安提供工控資安輔導，工研院量測中心驗證，TÜV SÜD 發證