萬物聯網，資安新主張

■文：任芷萍

照片人物：力旺電子 (ememory) 創辦人暨董事長徐清祥

「資安」可謂是數位化轉型的全民公敵。力旺電子 (ememory) 創辦人暨董事長徐清祥日前在《CadenceLIVE Taiwan 2023 使用者年度大會》揭示萬物聯網時代，資安風險如影隨形，有三大隱患：一是連結端點變多，從 1993 年電腦互聯網、2009 年擴及到人、2023 蔓延到物，意味駭客的攻擊面也變大；二是應用多元，在人工智慧 (AI)、機器人、軟體定義、永續設計 (Sustainable Design) 等加持下，物聯網 (IoT) 正深入每一個角落，資安威脅無所不在；三是連網裝置的生命週期越來越長，產品設計之初若不將安全納入考量，之後恐面臨更大的問題。

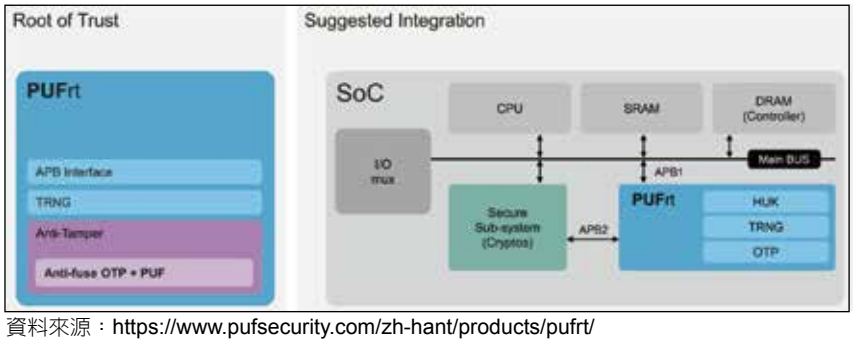
徐清祥直言，顯然，過去僅仰賴軟體保護系統的方法已不可行，硬體勢必也須參與其中；那麼，是要採用 HSM (硬體安全模組) 或 TPM (信賴平台模組) 晶片把關？還是將它們轉成 IP (智財權) 形式、直接內嵌到每個晶片裡？端視應用而定。例如，電動車對晶片安全要求相當嚴格，從閘道器 (Gateway)、控制器 (Controller) 到邊緣裝置的晶片，皆明訂須內嵌安全功能。就系統觀來看，杜絕供應鏈出現仿冒元件是首要任務；美國力主落實供應鏈本土化的動機之一更是基於安全考慮，尤其是關乎國家安全的應用，零信任 (Zero Trust) 等級更是必備條件。

力旺&熵碼科技：PUF-based 信任根建構獨特晶片指紋

此外，還須從硬體著手保護數據的處理、儲存、使用，並確保正版應用軟體未被竄改過，才有足夠能力抵抗駭客攻擊。徐清祥透露，當今仿冒品猖獗，每年約有超過 750 億美元的半導體元件營收是被其所剽竊而得；只須花台幣千元的成本購得板子就可側聽加密過程、對金鑰進行解密；軟體更新也存在風險，一旦被竄改就可能取得系統掌控權。總之，半導體元件、裝置硬體、用戶端軟體安全之於系統防護缺一不可；與此同時，透過指紋為機器與人或應用之間做安全防護是最根本而有效的，晶片亦是如此。

力旺藉由自家非揮發性記憶體 (NVM) 技術，攜手子公司熵碼科技 (PUFsecurity) 共同開發 PUF-based (物理不可仿製功能，Physical Unclonable Function) 之硬體信任根 (ROT)——PUFrt，在原有 OTP (一次性可編程) 基礎上整合為次系統 IP 作為晶片指紋，

圖 1：UFrt 硬體信任根為系統安全提供堅實基礎，打擊反向工程並徹底改革設備認證方式



資料來源：https://www.pufsecurity.com/zh-hant/products/pufrt/

為裝置的操作完整性與信任提供理想保護。徐清祥指出，安全系統的核心是：儲存及產生鑰匙，以搭配加密引擎確保裝置安全運作——應用韌體 (Firmware) 及軟體驅動處理器執行簽章、認證及數據加／解密工作，且須經有 ROT 鑰匙保護的演算法檢驗，才能防範駭客從演算法回推運算邏輯。

反熔絲 OTP，讓駭客根本找不到金鑰所在！

徐清祥宣稱，目前全球每年約有 900 萬片、約 11% 的晶片有用到上述 IP 產品，旨在取代傳統的 eFUSE—— 可動態即時地重新修改積體電路 (IC) 中的程式，以便在出廠後運作時，仍可再針對晶片性能做調校，兩者的最大區別在於信任規則 (Rule of Trust)。相較於 eFUSE 是用燒斷導線方式來判別 0、1，基本上電路分佈形態仍固定可見，僅能訴求讓反向工程無從辨識存放內容；反熔絲 OTP 是透過電磁很強的高電場改變電晶體氧化層原子架構，原子鍵結變化會造成很小區域、幾乎看不出來的漏電，讓駭客根本找不到鑰匙存放的確切位置，相對更安全。

他繼續揭密反熔絲 OTP 工作原理：將電晶體氧化層的散亂結構在電路上呈現，並將「亂度」萃取出來變成電訊號以作為晶片指紋。當原子鍵結斷掉、電流就會增加，但相鄰的兩個電晶體，卻讓人不知道哪一個會有較大電流產生、又是哪一個完全不會產生電流；若將多組類似成對的電晶體放入一個矩陣、形成亂數 (實驗可達百萬常數)，借助如此超長度的密鑰並攪和、分散存放位置，甚至可阻擋量子電腦的攻擊。結合運算電路及外來雜訊 (本身又是一種亂數) 混成亂數產生器，可讓駭客完全摸不著頭緒，可滿足所有半導體元件的安全需求。

從 IC 出廠到裝置 EOL，嚴密保護系統

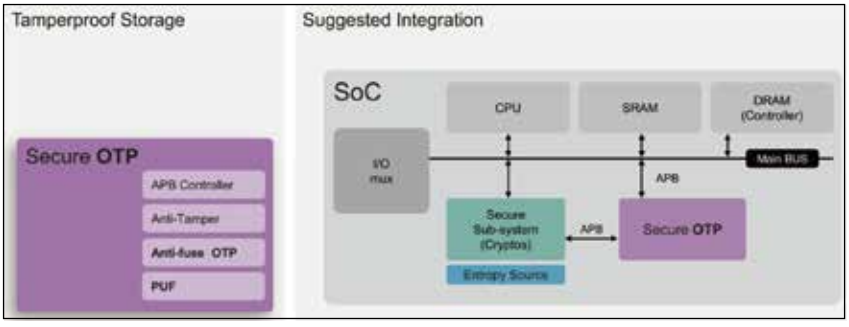
他強調，PUF-based 的 OTP IP，從 IC 出廠、執行運算、到裝置整個產品生命週期結束，皆可確保系統受到嚴密保護，且架構面積僅 0.15mm^2，僅佔總體晶片成本非常低的份額。他並提醒，時至產品生命週期終了 (EOL)，要記得把身份認證 (ID)、公鑰證書等關鍵資訊刪除，以免有心人士惡意備份、借屍還魂；以汽車先進駕駛輔助系統 (ADAS) 為例，在裝置就緒 (Device on Board) 後，會經由獨一無二的 ID 及鑰匙產生器進行授權、公／私鑰交換，才會執行後續數據收集、儲存、傳輸，以及分析、模擬、評估等模型優化工作，最後予以調整數據。

徐清祥陳述，以往，所有元件皆透過集中式控制器 (Central Controller) 掌控數據進出，安全措施亦統一由閘道器負責，未必需要每個元件都內嵌安全功能，但相對的，只要有一個元件被駭，所有裝置都將曝露在高度風險中；尤其今天的汽車動輒內含上千個電子元件，威脅著實不可小覷。為免互相拖累，最佳方式就是每個元件的晶片皆有獨立安全裝置，也更符合零信任架構精神。最後他總結，當網路安全 (Cybersecurity) 風險與日俱增，從供應鏈、裝置本身到應用端的整個生態系的安全防護更須嚴謹，惟有 PUF-based 硬體信任根可滿足所有需求。

關捷公司：資安觀念由保護網路，轉變爲保護資料／應用

聚焦於金鑰管理的關捷公司，對於 IoT 設備與 HSM 應用實務亦有一番見解。執行長洪伯岳表示，IoT 時代，每個裝置都需被賦予一個身分，以確保連網設備及交付資料的正確性；為此，行動資安聯盟、

圖 2：透過安全的反熔絲 OTP 來保護靜態數據



資料來源：https://www.pufsecurity.com/zh-hant/products/secure-otp/


照片人物：關鍵公司執行長洪伯岳

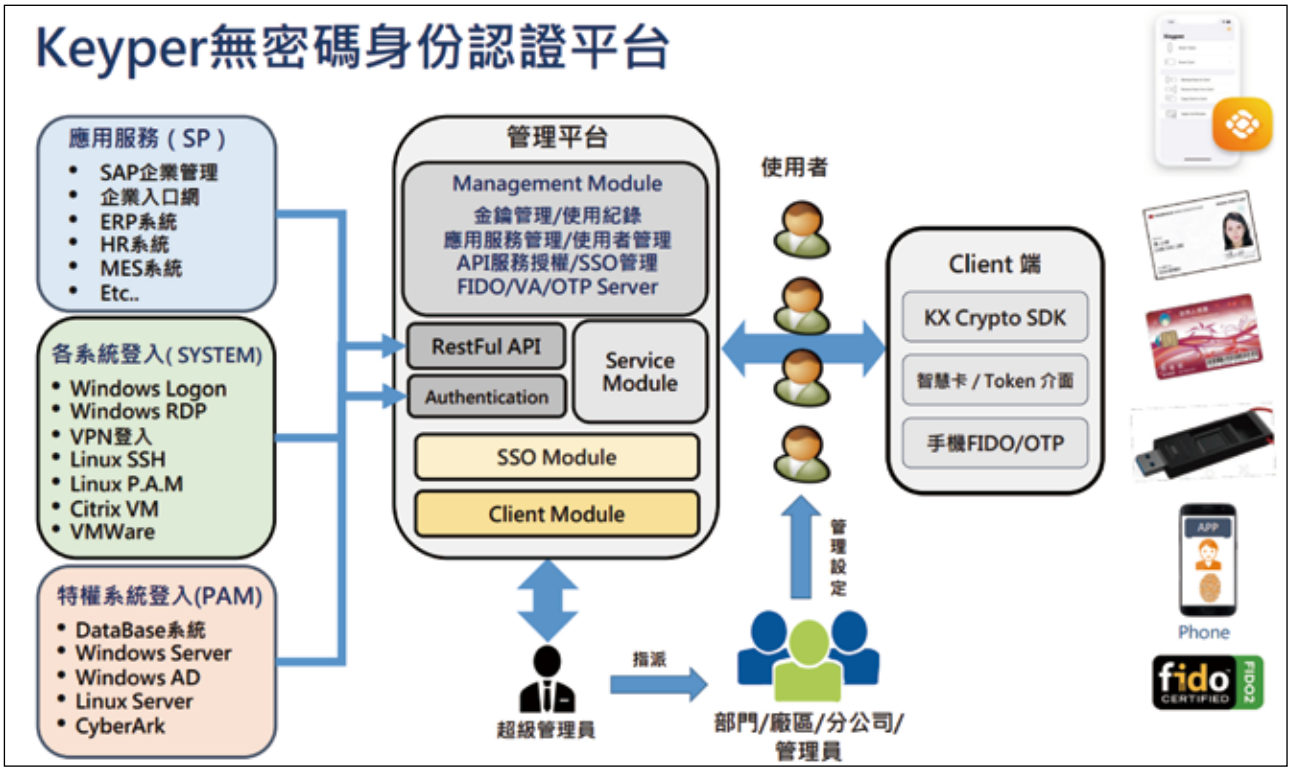
台灣資通產業標準協會 (TAICS) 等業界組織已陸續推出若干 IoT 資安標準。對於設備身分認證來說，最重要的就是確定產品金鑰的唯一性，韌體的更新路徑亦須加密，然後再到中央處理器 (CPU) ／微控制器 (MCU) 解密；以智能車為例，當中所有主動式感測器都必須有獨立身分、產生相對應的金鑰，以便未來無人車可追溯相關責任。

於是，資安觀念也由保護網路存取轉變為保護資料／應用存取，「零信任」概念亦由此誕生，不僅落實在製造生產，還須達到每一個步驟都永不信任且必須驗證，而 ROT 是在網路世界中始終可以信任的來源。他強調，對資料進行加、解密並執行生成數位簽章和驗證簽章等功能的金鑰，不能被保存在開放的作業系統 (OS) 或雲端，才能達到不可否認性並避免內部威脅。為保護晶片安全，通常會使用 ROM 帶有公鑰的安全開機以免被注入惡意程式碼，只有正確簽章的程式碼才能運行——用於簽章的金鑰被儲存在 HSM，受到嚴格管控且在生產環境中不可用。

資安四大屬性：保密性、完整性、可用性、不可否認性

因此，攻擊者幾乎不可能為被竄改的影像生成正確簽章。洪伯岳說明，HSM 本身就是一個安全晶片 (Secure Chip)，是可獨立進行密鑰生成、加解密的可信任平台模組，有自己的安全記憶體儲存區域並運行自己的微型 OS，可用於儲存密鑰或特徵數據，能為智慧手機、電腦、IoT 等電子設備提供加解密和安全認證服務，晶片金融卡即是此類；HSM 內建密碼演算法加速器及安全儲存空間以保護金鑰和敏感資料，通常具備國際安全認

圖 3：關鍵公司 Keyper 管理功能包括——使用者權限分配、驗證機制、設備／網頁訪問控制、驗證服務、稽核記錄



資料來源：關鍵公司

證——眼下以北美市場的 FIPS 140-3 認證和歐洲的 ISO 15408 (CC) 認證為兩大主流，擁有偵測入侵及抵抗入侵的能力。

現今電腦都會內建 TPM 亦是同理，在本機產生私鑰 (private key)、達到唯一性。洪伯岳歸納出資訊安全有四大基本屬性：保密性 (Confidentiality)、完整性 (Integrity)、可用性 (availability)、不可否認性 (Non-repudiation)。洪伯岳還提到：現正力推的 FIDO (Fast IDentity Online) 等無密碼身分認證若設備遺失恐面臨無法登入任何系統的窘境，此時，平台的身分認證管理就格外重要，關鍵公司因而投入身分認證／身分授權、資料加密、生物辨識、FIDO 等安全令牌 (Token) 的開發，已獲台電智慧配電身分認證系統、銀行客戶單一簽入服務專案等採用。

圖 4：「加密勒索攻擊」手法示意

資料來源：中華資安國際

中華資安國際：「加密勒索攻擊」是最大威脅！

致力於事前檢測、事中監控應變、事後鑑識回復之「一站式」資安服務的中華資安國際 (CHT Security)，從自家去年資安事件處理統計結果發現：「加密勒索攻擊」是智慧製造場域所面臨的最大威脅，尤以亞太區為甚；抓住製造商無法忍受停機導致上千萬美元損失的心態，使勒索成為攻擊者一個有利可圖的手段，此種攻擊是許多場域主的夢魘，因為往往伴隨著資料外洩的風險。

照片人物：中華資安國際鑑識暨健診部經理劉叡

中華資安國際鑑識暨健診部經理劉叡解析，惡意程式類型以 Webshell 的 31% 居冠，Hacktool、Loader 各以 14% 並列第二；駭客入侵手法 (Initial Access) 以源於服務介面／設備的「開採對外應用」(Exploit Public-Facing Application) 為大宗，包括：企業官網、公文交換系統、電子郵件、未經保護的物聯網 (IoT) 設備等，尾隨其後的駭客途徑是有效帳號 (Valid Accounts) 和路過式攻擊 (Drive-by Compromise)。其中，前三大公開漏洞則是：上傳漏洞 (57%)、SQLi 漏洞頁面 (26%) 及身份認證漏洞 (4%)。依中華資安國際 IR 案例統計與 Gartner 2023 網路安全趨勢報告，劉叡建議有三大課題須嚴陣以待：

- 威脅暴露管理 (Threat Exposure Management)：對外服務介面存在弱點或未妥善控管；
- 身分識別架構免疫 (Identity Fabric Immunity)：存取為未授權使用者及裝置；
- 網路安全驗證 (Cybersecurity Validation)：企業組織建置的「縱深防禦」的網路安全防護有效性。

連網造成破口，「資安防護四防線」應戰

劉叡表示，針對以上課題加上因應智慧製造的關係，許多 OT 設備已連網，可能造成防禦破口，中華資安國際提出「資安防護四防線」強化資安：

1. OT 資安健診：了解工控系統 (ICS) 潛在風險，如架構弱點、場域端點、網路流量是否異常？找出高風險關鍵資產，判斷風險影響範圍，搭配弱點掃描進行修補，建立安全網路架構；
2. OT IDS/IPS(入侵偵測系統／入侵防護系統)：於場域中建立威脅感測器，部署入侵偵測／防護系統偵測或阻擋惡意活動等網路流量安全機制；
3. OT SOC(資安監控中心) 監控：7x24 監控安全與隔離性，收集告警紀錄以應變處理；
4. IEC 62443 制度導入：建立工控網路安全營運計畫。

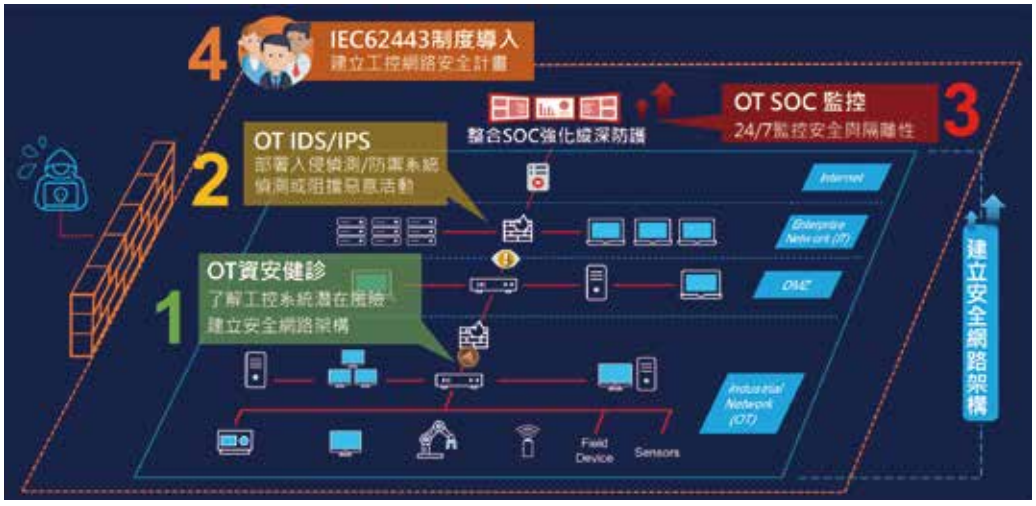
如此，亦可與 SEMI E187/E188 半導體資安標準有所呼應。中華資安國際是從中華電信獨立出來的專業資安服務公司，旗下「數位鑑識暨資安檢測中心」已於 2020 年 12 月 14 日取得 ISO 17025 認證，為 TAF (財團法人全國認證基金會) 認可實驗室，可提供資安事件應變處理、數位鑑識／IoT 檢測、惡意程式快篩、IR 應變能力建置等服務。以 OT 資安健診為例，除工具提供之防護資訊、專家評估外，還參考國際工控資安標準「NIST 800-82 Rev. 2」、「IEC 62443」與主管機關規範給予改善建議。

資產擁有者／服務提供商、系統整合商、產品供應商，各有對應法規

OT IDS/IPS 主要作用是做「隔離性監控」(未授權資產上線、幽靈網際網路連線) 與「惡意行為監控」(攻擊行為、掃描行為)，兩者差別在於：IDS 用於入侵偵測的軟、硬體，針對網路與系統間的通訊行為，進行收集分析、比對與研判，若偵測到異常行為，可自動發出告警，通報資安人員與場域管理者；IPS 意在即時攔阻威脅及區隔資產，提升 OT 場域網路防護與阻擋能力，並利用虛擬修補 (Virtual Patch) 減低漏洞修補及維護所需停機時間，以配合全天候運作的生產程序。另搭配惡意程式檢測 (Malware Scan) 的 OT SOC 監控日益受矚，Malware Scan 也是 SEMI E188 關注焦點。

劉叡指出，OT SOC 監控服務可即時偵測威脅，防堵災損擴大，若搭配資安事件應變能力建置服務，可基於 OT 場域現有資安事件應變 (IR) 制度架構，參考 NIST SP 800-61 Rev. 2 定義的事件回應生命週期，分別是「準備」、「偵測」、「分析、遏制、根除和復原」與事件後活動，協助客製化符合場域需求之 IR Playbook (類似教戰手冊) 並執行 IR 應變演練，透過桌上型推演或模擬環境攻防，以提升企業資安應變能力及熟悉度。最後不容忽視的是國際法規要求：資產擁有者／服務提供商 (IEC 62443-2-4)、系統整合商 (IEC 62443-3-3)、產品供應商 (IEC 62443-4-1/IEC 62443-4-2)，訴求產品須經過檢測且確保有安全的開發程序。

圖 5：智慧製造場域資安防護四防線



資料來源：中華資安國際

智能車資安風險升高，ISO 21434/ISO21448 新規上路！

■文：任芷萍

照片人物：SGS 功能安全暨資通安全服務中心技術經理及功能安全專家張國樑

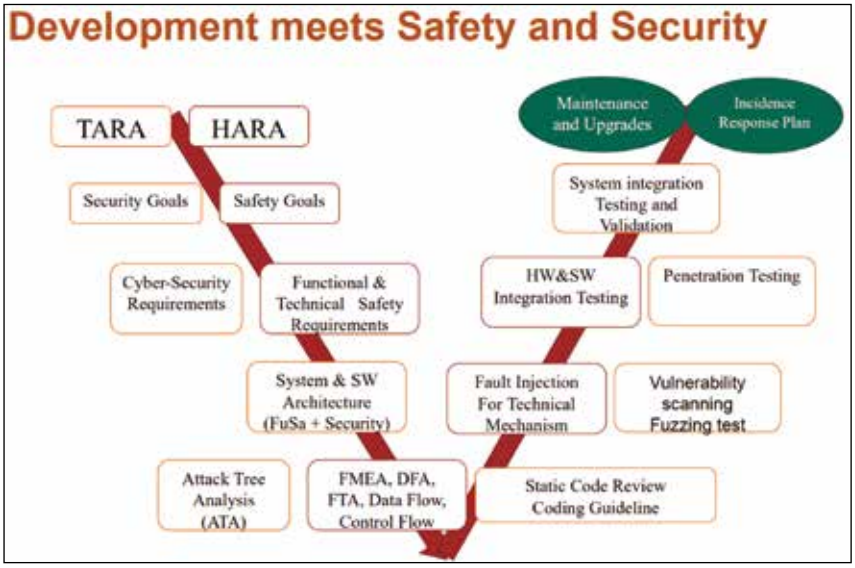
汽車趨向智慧化，自然而然亦成為資安重點防禦範疇。SGS 功能安全暨資通安全服務中心技術經理及功能安全專家張國樑表示，由於客戶端拉動，汽車電子廠商不得不日益重視信賴性 (Dependability) 等國際標準，業界期盼有一套「多合一」的方法分析與共通的開發流程以應對上述要求，並融入企業文化中。以此為前提，下有六大支柱：功能、效能 (可用性)、可靠 (耐用)、功能性安全、網路安全及預期機能安全 (SOTIF)，需要 IEEE 標準支援技術開發，為產品的設計驗證提供框架。

SGS：汽車資安新規 ISO 21434，可與 ISO 26262 做標準融合

例如，ISO 26262 聚焦的是故障 (Fault)——透過流程降低系統性故障、經由保護機制的設計來避免隨機性故障，因為故障、錯誤及失效會威脅到信賴性，通常會以防止故障、故障容忍 (容錯系統)、故障移除、故障預測等手段來加以杜絕。十年前 ISO 26262 的出世，提供系統化方法做新技術的設計驗證；以此為基礎，2021 年出爐的 ISO 21434 鎖定的是資訊安全，ISO21448 (SOTIF) 則是為自駕車而準備。歐盟算是最早對於汽車的資安有實際作為的區域市場。

R.155 / R.156 強制規範進口到歐洲的 Tier1 車廠皆須確保汽車的網路安全及 OTA (空中更新) 管理系統，且必須透過第三方認證；但由於規範內容過於空泛，使得 Tier2 以下的供應商在實務上有執行困難，ISO/SAE 21434 便是在這樣的機緣下誕生，且現正制訂相關稽核標準——ISO PAS 5112。

圖 1：符合汽車安全性與資安的開發模型



資料來源：SGS

ISO 21434 著重於須依編碼指引做程式碼的靜態分析、規則檢查、漏洞掃描、滲透測試等，與 ISO 26262 在立法精神上有多處重疊，因而省略許多流程細節的規範，且許多方法論都可與 26262 對比，借助標準融合 (Standard Fusion) 以期達到省時省力。

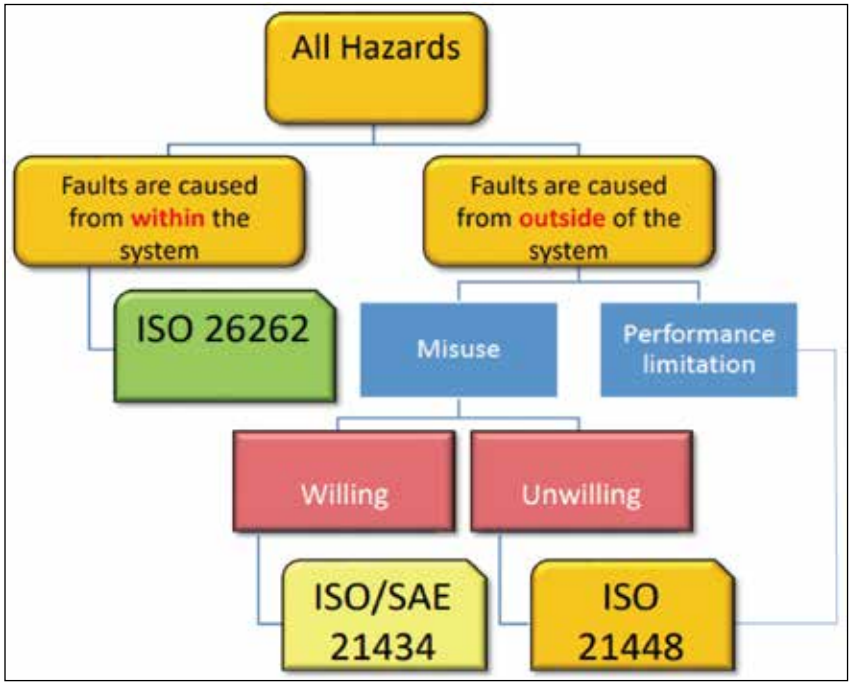
張國樑建議，廠商若同時要符合兩種規範，可在功能安全文件就緒後，就技術層面和系統級別推導出基礎系統架構，分析、評估是否存在資訊安全的威脅 (Threat Analysis and Risk Assessment, TARA)，進而推導網路安全要求。從系統觀來看資安的軟體層級，識別出網路安全的要求後，就能清楚掌握細部規範，例如，傳統通訊網路會要求晶片上要有控制器區域網路 (CAN Bus)，那麼，軟體如何編寫通訊協定與電子控制器 (ECU) 溝通？以及 CAN 規定須做加、解密以確保資料的完整性，要如何儲存、處理數據？加、解密要複雜到何種程度，採對稱型或不對稱型？

安全系統認證須具備「可追溯性」

張國樑繼續陳述，效能、有效性、加解密時間都須經過驗證，包括：網路安全措施有無潛在限制？來自外部、內部的威脅？法規測試／安全分析要求？另由於加解密過程有一定耗時，是否所有用例皆須賦予高規格？ MISRA C:2012 三版 (MISRA C 是由汽車產業軟體可靠性協會所提出的 C 語言開發標準) 與 CERT 有效靜態分析即是針對符合資安要求而訂定。「Well-trusted cybersecurity」(可信賴的網路安全) 對於 ECU 設計十分重要，控制方法有以下幾種：密碼演算法、加解密硬體加速器 (單晶片硬體安全模組或引擎)、密鑰儲存、身分識別機制等。

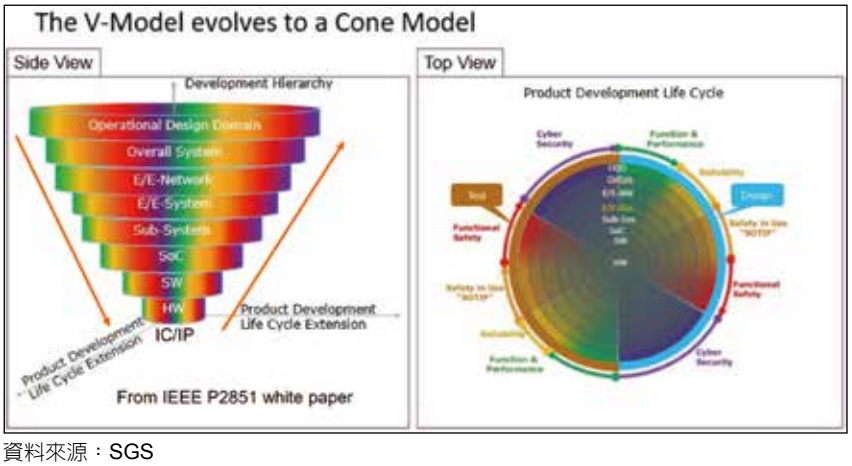
之後的測試方法與深度，亦是工程師最大的挑戰，從軟體網路安全需求、設計到導入須具備「可追溯性」。新近問世的 ISO21448 (SOTIF) 亦是 ISO 26262 的延伸，著眼於意外誤用、感測器／致動器／演算法性能極限等外部故障；簡言之，26262 關注的是系統失效，SOTIF 側重系統弱點。供應鏈的數據交換模式也因為須融合、共同統整規劃，從傳統的 V 字型視角 (V-Model) 轉為立體的圖錐形視圖

圖 2：SOTIF 在汽車系統安全生命週期的對應關係



資料來源：SGS

圖 3：汽十供應鏈數據交換模式的轉變



資料來源：SGS

(Cone Model)，礙於時間、成本壓力，面對所有需求必須有所妥協，不可能全部做滿，另須思考的是：相同的分析方法是否能用於不同標準？彼此是否存在橫向關聯性？

投入嵌入式系統屆四十年的愛亞系統 (IAR)，從軟體開發的角度剖析在獲得功能安全系統認證 (工具認證) 不可忽視的重點。資深技術經理及功能安全專家蔡本中指出，在 ISO 26262 概念到生產的整個開發流程可看到系統、硬體、軟體三個 V-Model，對於工具使用亦有相關規範，第八章詳列置信度等級 (Tool Confidence Level, TCL) 有兩大參數：TI 關注的是工具是否會對開發產生影響——TI1：無影響、TI2 有影響，TD 瞄準工具錯誤檢測，乃指防止／檢測工具發生故障並產生相應錯誤輸出措施的信心——TD1：高度信心、TD2：中等信心、TD3：其它情況。

IAR：開發工具攸關「置信度」的判定&解套

例如，編譯器 (Complier) 絕對會影響置信度的判定，就落在 TI2 區塊；而最糟的情況就是 TI2 與 TD3 的矩陣交集：TCL3。此時，開發工具的選擇將是關鍵，有四個解套方式：

- 1a：提出工具已被車用開發使用過 (實務上較不可行)；
- 1b：提出工具開發流程的評估 (實務上較不可行)；
- 1c：使用測試套件驗證工具 (需要投入人力資源)；

照片人物：IAR 資深技術經理及功能安全專家蔡本中

- 1d：使用安全標準開發的工具。

相較之下，1d 是四個選項當中可行性最高者，IAR EW/BX 工具便是由此而生，標榜通過業界最多的認證標準，不僅可滿足 ISO 26262 車用產品所需，亦能符合 IEC 61508 工規產品、IEC 62304 醫療產品要求。其中，整合靜態分析工具 (C-STAT) 和動態分析工具 (CRUN) 可有效提升程式碼品質，與 ISO 21434 資安議題尤其高度相關：1. 在最初開發階段部署，有助改善除錯曲線；2. 可在不改變開發過程下，完美集成到 IAR Embedded Workbench 開發環境，在日常開發中使用；3. C-STAT 支援嵌入式開發中實用的編碼標準，如：MISRA C/C++、CWE、CERT C/C++。

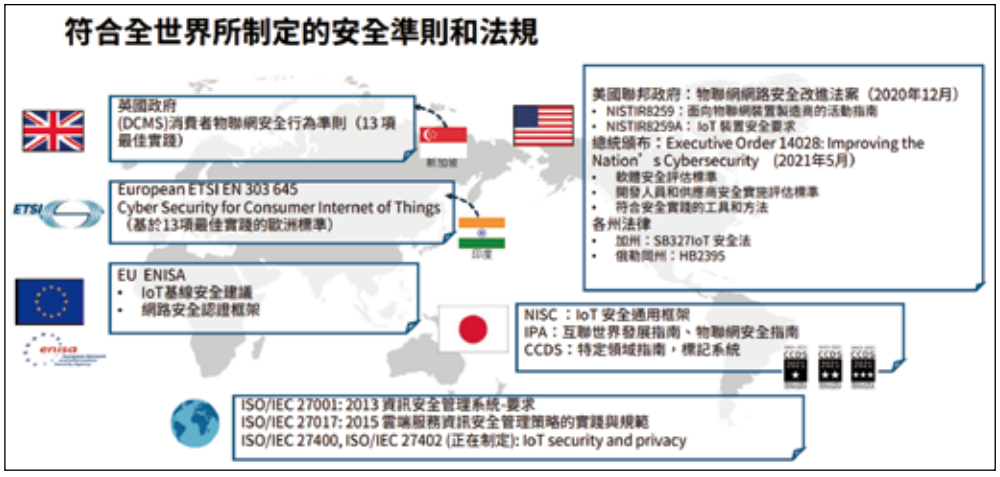
蔡本中表示，汽車開發對於開發工具的品質極其重視，使用靜態分析工具 C-STAT 不僅可掃瞄程式碼是否合規、設定編碼規範找出潛在隱患，還能明確指出哪一個 .c 檔的哪一行程式碼有誤，開發者可透過詳盡的說明文件了解程式碼規範，並有程式範例可供參考，另提供命令列模式可輕鬆整合 CI/CD。另一方面，對於變數初始化、字串和指標的使用需更加謹慎，以免造成安全漏洞，而 CERT 規範可檢查程式碼以增加安全性。此外，使用動態分析工具 C-RUN 可查找運行時才會發生的問題。

嵌入式安全應秉持「Security Made Simple」

不用事先設置任何斷點，在運行時自動檢測出程式發生的記憶體越界存取、變數溢出等問題，支援最貼近產品實際運行條件的獨立模式，如：Heap 為動態記憶體配置區域，C-RUN 可檢測超出 Heap size。蔡本中提醒，通常看似平常簡單的程式碼，卻可能隱藏著非預期的錯誤發生，可正常編譯亦沒有任何報錯、人為檢視也不容易發現錯誤；而 C-RUN 可協助運行到該行程式碼時中斷並報錯。ISO 21434 重點關注組織中產品開發的網路安全流程和最佳實踐，涵蓋廣泛、但僅限於與嵌入式設備相關的特定部分，且還需要後端系統支持。

蔡本中認為，嵌入式安全應秉持「**Security Made Simple**」原則以應對與日俱增的物聯網 (IoT) 安全威脅，有效避免 IP 盜竊、偽造和生產過剩等攻擊，而如何因應各國制定的安全準則和法規亦是重點對此，IAR 除了積極與多家車

圖 4：全球陸續頒布關於資安與網路安全的準則／法規



資料來源：IAR

圖 5：IAR 幾乎可實現嵌入式應用的所有安全實作準則

資料來源：IAR

用工具或第三方廠商進行整合，並擁有三大法寶備戰：

1. 合規性 (Compliance)：以符合各國制定的安全準則，實作嵌入式程式的安全保護機制；
2. 多支援 (Multiple Support)：搭配各大廠牌的微控制器 (MCU) 硬體安全功能，輕鬆整合於原本的程式開發流程並支援各家 IDE (整合開發環境)；
3. 端到端 (End-to-end) 解方：提供從程式開發原型，到產品量產安全燒錄最完整的解決方案。

就開發週期來看，IAR 提供兩種嵌入式 EMB Security 解方。首先是完整端到端的 Embedded Trust (ET)，主打身分鑑別 (Authenticity) 及防版本回滾 (Anti-rollback) 功能，涵蓋安全需求、安全啓動管理、開發軟體應用程式、軟體測試全流程，將安全化繁為簡；若已進入後期開發階段、前期皆未及建立安全機制，則可以 eSecIP 做主動智財權保護 (Active IP Protection) 及反克隆 (Anti-cloning)，將原有程式連接 Security Service Library 進行加密保護，以 JSON 檔案進行相關安全設置並透過 OrBIT 命令列產生量產生產包，最後將量產生產包進行安全燒錄。

最後，蔡本中統整 IAR 對於車用開發的核心優勢在於：1. 提供最完整的「5S」(Size/Speed/Safety/Security/Support) 嵌入式開發的解決方案；2. 功能安全版本可滿足長期開發維護需求，並優先處理遇到的技術問題；3. 可化繁為簡保護 IP，提供端到端 (ET) 或後期 (eSecIP) 的安全保護 (參閱：《從 IP 到生產，產品認證履歷必備！ IAR 為嵌入式系統「端到端」安全設計奠基》一文 http://www.compotechasia.com/a/tactic/2023/0825/55318.html)。

CTA

力阻火燒連環船！製造業「供應鏈資安」環環相扣

■文：任芷萍

照片人物：睿控網安 (TXOne Networks) 首席解決方案架構師劉大川

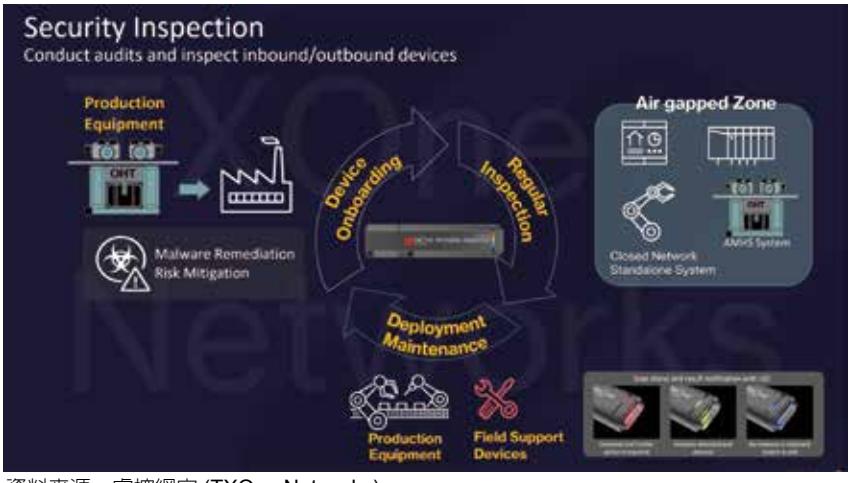
日前在《SEMICON TAIWAN 2023 國際半導體展》上，幾位熟稔智慧製造資安的專家也針對相關議題分享看法。睿控網安 (TXOne Networks) 首席解決方案架構師劉大川表示，工業資安影響最為巨大的當數供應鏈供擊，製造業資安事件有半數 (近 47%) 是因新購設備進廠前未確實完成安檢、致使自帶威脅進入場域而觸發。台積電 (TSMC) 2018 年爆發重大資安事件後，2019 年開始推動 SEMI E187 法案，它亦是首個由台灣主導之半導體產線設備資安標準規範，旨在訂立新進設備在進廠前的安檢程序和規範是否有符合資安要求。

睿控網安：生產場域網路須有「隔水艙」設計

劉大川點出這意謂：供應商在交付機台前必須把資安提到某個水準之上，這與美國去年力推的網路安全構想不謀而合。與其為待售機台外加許多資安防護，倒不如從設備設計之初就把資安納入考量，並在進廠前、例行性維修、歲修維護期間皆須做安檢，以確認任何改變、更動、移置機台的行為皆不會讓病毒有任何可趁之機。以往，在機台進廠前的掃毒健檢標準程序是：拆機殼、裝光碟機和防毒軟體，待掃描完成再移除光碟機、裝回機殼，然而麻煩的是，一旦機殼拆了後再裝回去就需重新校正，曠日廢時。

劉大川解析，一個變通方式是利用 USB 裝置進行掃毒或弱點評估，之後再出具符合 SEMI E187 的合規報告。評估要項包括：作業系統 (OS) 是否過期？機台是否存在弱點？其中有無潛藏病毒？以上規範皆須符合，且機台必須安裝防毒軟體才得以進廠。但在實務上，若考慮到機台資源有限、安裝防毒軟體恐影響效能，則至少要羅列「白名單」(Trust List)，強制二擇一；更不允許早期連登入帳號、

圖 1：新購機台設備進廠前須經安全檢查



資料來源：睿控網安 (TXOne Networks)

密碼都沒有控管，開機就能運作的情況發生。另一個由英特爾 (Intel) 主導的規範 SEMI E188 則是為減少惡意軟體傳播到製造設施、並在製造設施內傳播定義框架。

他深入剖析，SEMI E188 有兩大主要精神：首先，生產場域的網路須有「隔水艙」設計，以免不慎破了一個小洞就可能拖累整艘船沉沒；TSMC 在經歷 2018 年資安教訓後，TXOne 隨即在隔年配合 TSMC 開發「隔水艙」公共等級的防火牆。與一般防火牆最大的區別是：除了對外連網的控管外，還將工廠內的可編程邏輯控制器 (PLC) 等作業機台身分認證、讀寫權限及通訊協定列管。(參閱：《防毒如防疫，工控資安需做好區段隔離＆邊界管理》一文 http://www.compotechasia.com/a/opportunity/2021/0823/48826.html)

新購生產設備三原則：進廠安檢、端點防護、網路切割

其次是老舊弱點屏蔽問題；以前還可用事後補丁 (Patch) 處理，但自從 E187 明訂新機台掃描完、若發現重大弱點必須修復後方能進廠，此法已不可行。為周全起見，特別在正式條文之外的實務指引明訂：中階以下的設備對於低階弱點要有屏蔽及補償措施，一言以蔽之，進廠安檢、端點防護措施、網路切割 (Segmentation) 是三大原則。E187 要求的是的 baseline

圖 2：SEMI E187(白字)——Secure by Design vs. E188(黃字)——Secure by Operation

資料來源：睿控網安 (TXOne Networks)

(基本準則，至少要做到才能進廠)，在產品設計階段就要把資安思維內化到其中，例如，人機介面 (HMI) 要有帳號密碼控管、內部規格要有資安考量、資料流對驗證有無限縮、對使用者的授權……。

從生命週期的角度來看，從設備製造商的設計到客戶端進廠配置、配方、強化端點，再到後續維修，聚焦的是「Secure by Design」觀念。劉大川繼續剖析 E187 有四大構面：不能使用過期的作業系統、網路須使用加密通道、終端端點要有防護、要有稽核軌跡。E188 著重的是「Secure by Operation」，不僅網路要做 Segmentation、隔水艙，生產設備端點經過任何變更、改變、維護、升級再回到產線之前，都須再做一次掃毒，確認「Malware Free」(沒有惡意軟體、病毒)，但沒強制要安裝防毒軟體。

劉大川補充，有鑑於條文未明列時間點的定義，為免爭議，SEMI 近期即將出爐的「落地指引」檢核名單會增列時間因素，載明多久時間以內的病毒碼或掃毒程序才有效？作業系統的效期？另端點若是選擇採用但在實務上，若考慮到機台資源有限、安裝防毒軟體恐影響效能，則至少要羅列「白名單」，以預載最佳，可減少許多整合測試等不必要麻煩，並須文件告知這些防護措施不會影響機台效能。成立於 2003 年、最早投入弱點掃描、同時著墨端點資安與物聯網資安解決方案的中華龍網 (DragonSoft)，則針對「供應鏈資安與零信任」提出見解。

中華龍網：「零信任」意即永不信任、持續驗證

中華龍網總經理孫建興直言，2018 年 TSMC 機台遭到勒索病毒感染、導致營收損失新台幣 52 億元一事，確實是喚起世人對於半導體供應鏈資安重視的轉折點；去年輝達 (Nvidia) 傳出遭駭客攻擊、被竊取大量資料的消息，又突顯了網路安全 (Cybersecurity) 的迫在


照片人物：中華龍網 (DragonSoft) 總經理孫建興

眉睫。事實上不只半導體，近年頻繁遭受駭客攻擊的產業供應鏈還包括：生命科學／健康照護、汽車、消費零售和能源。當系統整合商 (SI) 把產品推向企業，客戶端未必知道背後軟、硬體供應商身分；由於當中牽涉繁多，越往供應鏈下游走、可視性越差、風險越大，越難掌握是哪一個供應環節出狀況。

孫建興指出，軟體供應鏈攻擊模式有四大類：1. 軟體供應商本身就是攻擊者；2. 軟體供應商被攻擊者所駭，其軟體產品因而被埋入惡意程式；3. 軟體供應商的產品使用含惡意程式的第三方軟體；4. 軟體供應商的產品使用含易遭駭程式漏洞的第三方軟體。毫無疑問，所謂免費的有時反而最貴，開源軟體等第三方軟體本身即蘊含高風險值；它的版本管理機制通常相對鬆散，駭客有較多機會將惡意程式或程式漏洞植入常用的開源軟體套件。有鑑於此，不同產業除了訂有相關標準加以規範外，更重要的是做到「零信任」(Zero Trust)。

孫建興解釋，所謂的「零信任」指的是：永不信任、持續驗證，旨在讓正確的身分可以存取由正確程式碼授權的正確機器，並在正確時間與情境下，存取到正確的資料。NIST (美國國家標準暨技術研究院的前身為國家標準局) 對此訂有 SP 800-207 (ZTA) 零信任架構，核心組件欲存取內、外部資源皆須從嚴經過 PKI (公開金鑰基礎建設) 數位簽章或認證等審核，且要確保機器須合規、沒有潛藏已知資安問題；與此同時，政府正力推「FIDO」(Fast IDentity Online，金融行動身分識別標準化機制) 快速認證，將分為三個階段推行：

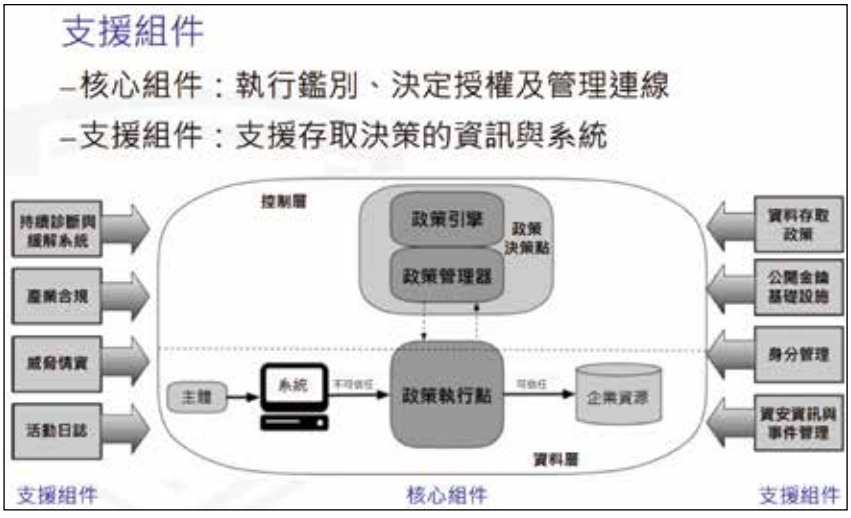
- 2022 年，身分鑑別：以生物識別鑑別器進行無密碼雙因子身分鑑別；
- 2023 年，設備鑑別：基於信任平台模組 (TPM) 之設備鑑別，並進行設備健康管理；
- 2024 年，信任推斷：依設備健康狀態、資安威脅情資及使用者情境等資訊，動態支援存取決策。

端點資安合規管理平台：以資產盤點爲基礎

「端點安全是核心，然後才有零信任和供應鏈安全可談」，孫建興強調。於是，中華龍網推出「端點資安合規管理平台」，以資產盤點為基礎，查核有無資安威脅？弱點？是否安全組態？作業系統／軟體是否合規？其中，又以下列三個面向最為關鍵：

1. 資訊資產管理 (IAM)：盤點政府／企業內部個人電腦及主機之數量、作業系統版本及配置部門等相關資訊，以利資管人員掌握場域端點及維運管理；
2. 電腦安全組態基準 (政府組態基準 GCB ／金融組態基準 FCB)：將政府／金融內部個

圖 3：NIST SP 800-207 (ZTA) 零信任架構



資料來源：中華龍網 (DragonSoft)；行政院國家資安研究院

人電腦及主機，套用符合美國 NIST 規範之一致性安全組態設定 (如：密碼長度、更新期限等) ，以降低遭駭客入侵之風險；

3. 軟體弱點管理系統 (VANS)：盤點比對政府／企業內部個人電腦及主機安裝之各類應用軟體已知的弱點或漏洞，進行修補更新，避免遭駭客利用，入侵企業網路及在內網橫向滲透。

孫建興進一步介紹 VANS 機制的目標是結合資訊資產管理與弱點管理，掌握整體風險情勢，並降低重大弱點爆發時可能造成之損害，包括：定期蒐集主機與電腦所使用之資訊資產項目及版本，建立資訊資產清冊，以達到降低風險與管控成本等目標，以及將資訊資產清單與弱點資料庫比對，以掌握所使用之資訊資產是否存在已公開揭露之弱點資訊。所謂的資訊資產涵蓋：應用軟體資產、應用框架、程式語言、應用程式中介軟體及作業系統，並揭示 TW GCB 發展規劃去年已將伺服器劃歸範疇。

他自豪地說，中華龍網不僅在 PC 端的 GCB 導入經驗豐富，伺服器的導入經驗亦優於其他廠商，且產品已經西門子 (SIEMENS) 等國際大廠認證，用戶遍及地方政府、桃園國際機場交通設施及金融證券櫃買中心，並統整中華龍網在 GCB/FCB 擁有四大優勢：

●完整售後服務：是台灣自主研發廠商，專案客製化能力強且彈性高；

●伺服器導入經驗豐富：提供逾十家客戶伺服器導入服務，例如：新北地政 (500 台以上規模)、合庫人壽、宜蘭縣政府等；

●稽核市占率最高：

◎政府體系——國內主要資安稽核廠商 (安碁、關貿、數聯、凌群、果核、漢昕)，均使用做為稽核各政府機關是否合規之工具；

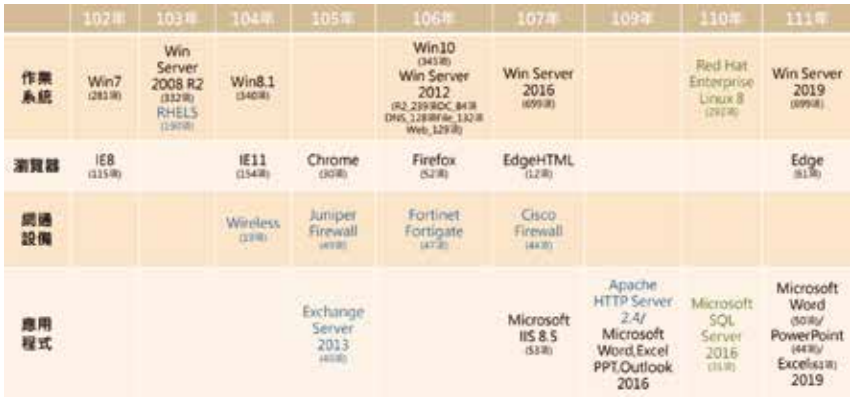
◎教育體系——為教育部 (資科司) 針對教育體系客製開發專屬稽核暨評量工具合作夥伴；

◎國防體系——為針對國防體系客製開發專屬稽核暨評量工具合作夥伴。

●Linux 稽核及導入服務：金融單位 Linux 導入服務、客製稽核工具 (用 CIS 做標準)，以及原廠服務支援。

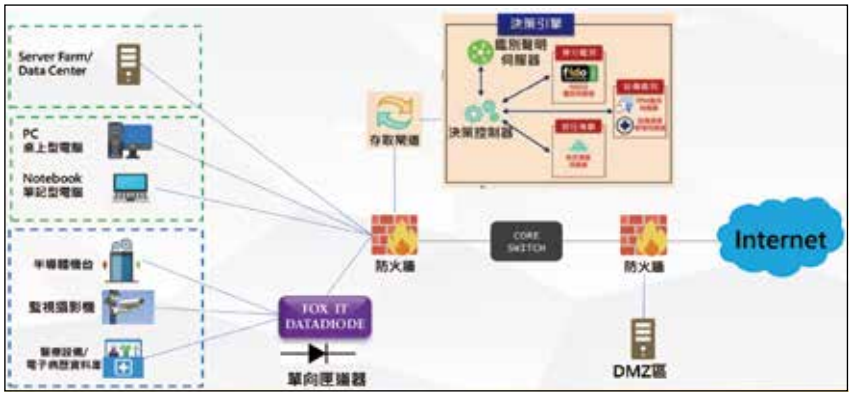
最後，他重申要打破內、外網概念，一律採「零信任」原則，即使是內部人員存取內部資訊也須經過認證，並強烈建議從 OT 場域丟出來的資料，最好走單向閘道器是最安全的方式——即使場域外有風險，也能有所緩衝、區隔；而整個 OT 環境最好維持對外封閉，不允許擅自安裝任何應用程式，將是最經濟有效的作法。更多訊息可參閱：https://www.dragonsoft.com/ 或 https://youtube.com/@dragonsoft4140?si=K6tGQ7ICux5QmQsm。CTA

圖 4：TW GCB 發展規劃



資料來源：中華龍網 (DragonSoft)

圖 5：中華龍網物聯網資安解決方案示意



資料來源：中華龍網 (DragonSoft)

無密碼 FIDO 落實「零信任」資安

■文：任芷萍


照片人物：數位發展部部長唐鳳

疫後生活、消費習慣急遽數位化，卻也讓網路詐騙有機可乘，日前由數位發展部 (簡稱：數發部) 數位產業署主辦的《2023 網路信賴基礎環境應用導入論壇》對於無密碼數位環境有深入探討。數位發展部部長唐鳳開場致詞：數位信任等同於數位韌性，密碼容易成為詐騙標的，惟有「FIDO」(Fast IDentity Online) 這種快速認證身分的機制才能建置真正的「零信任」(Zero Trust) 資安——包含生物特徵、設備裝置與連線行為是三道「防盜門」。數位發展部亦於今年 1 月加入國際身分辨識標準組織 FIDO 聯盟，目前台灣分會已有 27 個會員。

數位信任、數據隱私、網路安全，建構可信賴網路環境

數位發展部去年成立之初即率先採用 TWFidO (中華民國行動自然人憑證) 用來登錄內部網站、系統簽公文等，內政部今年 8 內亦修正通過「內政部行動自然人憑證系統介接申請要點」，擬將 TWFidO 系統的服務對象從原本電信、醫療等行業，擴大至行動自然人憑證系統、到適用個人資料保護法的機關或非公務機關。TWFidO 不只簽章、認證身分功能，它跟卡式的自然人憑證一樣，還有加、解密功能，惟現階段還在測試中；之後紙本公文可利用 TWFidO 進行端到端加密實現數位化，公務活動也可不必限於特定地點進行。

工研院資訊與通訊研究所副所長黃維中表示，可信賴的網路環境由數位信任、數據隱私與網路安全三者構成安全機制——數位信任是網路信賴的核心，又可概分為數位身分識別 (身份證明、驗證) 和簽章兩大塊；數據隱私保護著重於遮罩及去識別化；網路安全藉由軟體、防火牆、滲透測試等達陣。密碼技術存在已久，但它其實很脆弱：運算加速及人工智慧 (AI) 進步，讓它越來越容易遭到破解；而隨著網路釣魚活動的智慧化、組織化、平台化、服務化，厲害到可自動化破解雙因子認證 (2FA) 及 OTP (一次性動態密碼)，更為金融業帶來大規模災情。


照片人物：工研院資訊與通訊研究所副所長黃維中

「追本溯源，問題出在共享密碼的身分驗證機制，讓存放共享秘密的主機成為攻擊目標，驗證過程容易遭到中間人攔截和釣魚

攻擊——FIDO 就是為此而生」，黃維中說。他解釋，FIDO 是一種安全便利的身分識別機制，結合終端比對生物特徵，提升使用的便利性，且生物特徵、密鑰皆存放於裝置安全儲存模組，保障隱私與安全性；主機僅用來存放公鑰，能降低成為攻擊目標的風險，且使用非對稱式密碼技術，可完全防止中間人和釣魚攻擊。更重要的是，FIDO 是唯一符合美國 (SP 800-63) 與歐盟 (eIDAS) 國家之政府與產業「高」等級身分證之產業標準！


照片人物：Mercari 資安長 (CISO) 市原尚久 (Naohisa Ichihara)

FIDO Passkeys 可抵擋「釣魚攻擊」

黃維中說明，FIDO 除了符合國際規範 ISO 29115:2003 四個身分驗證與識別等級 (Level 1 ～ 4)，還同時覆蓋美國 NIST SP 800-63 (2017)、Revision 4 (2023) 明訂三個身分驗證等級、三個身分確認等級及三個身分聯邦等級 (皆分為：低、中、高三等)，簽章法規則有 ESIGN/UETA、NIST FIPS 186-5；而歐盟 eIDAS (2015) 有低／中／高，三個身分驗證及識別等級，eIDAS2 (2023) 則是簽章／進階／合格三個簽章等級。但他特別提醒：採用 FIDO 不見得就符合 NIST SP 800-63 或 eIDAS 規範！技術符合與取得認證是兩回事。

在 2019 年推出智能手機支付服務 Merpay 的 C2C 市集日本廠商 Mercari，就曾身受密碼所苦：容易被遺忘、破解、攻擊或洩露，且會被某些服務拒絕，因而決定採用生物驗證、密碼管理、簡訊 OTP 等多因子驗證 (MFA)。資安長 (CISO) 市原尚 (Naohisa Ichihara) 剖析，雖說 MFA 可強化使用者認證，但有些 MFA 用例仍透露不夠堅固的訊息，只有能「抵擋釣魚攻擊」(phishing-resistant) 的 FIDO 金鑰 (Passkeys) 是最佳解，並預言未來十年將快速成長——這是因為大約在 2020 年 FIDO 處於快速擴張期，FIDO2 與 WebAuthn 也開始擴散。

市原尚久指出，FIDO 發展大致可分為三個階段來看：2013 年由 UAF/U2F 帶頭、2019 年由 FIDO2/WebAuthn 啓動、2022 年後將由金鑰展開第三階段的成長。他並提到帳號恢復議題：當使用者購買新手機、或是設備遺失／被偷／損壞時，若要恢復程序，需輔以額外的 ID 驗證、認證及提示程序才行；此時，不良的使用者介面恐成大問題，甚至無法抵擋釣魚攻擊。FIDO 密鑰配對可作為多裝置憑證 (Credential)——可在不同裝置或瀏覽器之間同步運作，並經由谷歌 (Google) Password Manager 和蘋果 (Apple) iCloud Keychain 管理，冀可解決帳號恢復爭議。

防堵時下駭客，ZTA 才是根本解決之道！

露天市集技術處協理陳贊元陳述，以往資安防護只靠三招克敵制勝：政策、演練、稽核。首先是建立全方位的資訊安全管理，確保企業和客戶的數據安全；然後定期進行資安演練，包括漏洞評估、滲透測試、DDoS 模擬和紅隊演練，以增強資安意識和檢驗防護能力；最後進行資安稽核，評估現有資安措施的效果，以及潛在威脅。然而，要防堵時下駭客非法行動，傳統作為顯然已不足以應對，惟有零信任架構 (ZTA) 才是根本解決之道！事實上，OTP 簡訊發送即是 ZTA 入門手段之一，優點是立即見效且使用者體驗一致。


照片人物：露天市集技術處協理陳贊元

不過，OTP 有三大缺點：1. 使用量越大，費用越高，成本是變動的、不易控制預算；2. 仰賴電信產業，在控管上效果有限；3. 使用者購物流程會被打擾或中斷，影響消費體驗。陳贊元認為，未來資安防護有兩大走向：一是設置專責安全操作中心 (SOC)，不僅可強化入侵偵測，還能提供數位鑑識記錄留存；二是持續迭代 ZTA，不斷提升安全技術和保護措施，以保障企業和客戶的龐大資料安全。因此，「FIDO2 ＋ Passkeys」的組合拳，將是大勢所趨，擁有以下好處：

■使用體驗優，登入過程更簡便；
■無密碼傳輸，改採公私鑰驗證；
■成本合理，且趨近於固定成本；
■政策支持，數發部大力推動導入。

每年處理交易金額達新台幣 900 億元的藍新科技，對上述觀點亦表認同。藍新科技產品規劃處處長林承勳分享，他們確實觀察到電商客戶有加強身分識別的需求，但對於導入 FIDO 常遭遇「3 門檻＋1 難關」：

■導入的進入門檻：不認識 FIDO，無法想像導入價值，FIDO 註冊前的身分核驗難以選擇強驗證或弱驗證，缺少可依循的作業指引、擔憂導入後無所適從；
■應用的技術門檻：對身分識別服務信賴者 (RP) 與身分識別服務提供者 (IDP) 之間的技術實作不熟悉，對 RP FIDO 伺服器的建置、維護與管理沒有經驗，對 FIDO 與現行身分識別技術的分工、導入應用或服務方式欠缺完整想法；
■驗證的成本門檻：投入成本是最關鍵要素，導入 FIDO 的效益是否夠高是權衡重點，擔心 FIDO 發展的不確定性造成成本難估算，於是，「繼續觀望」便成了安全選項。

FIDO 應用擴至一般大眾的日常生活

「支付服務亦存在驗證難關」，林承勳說。這是因為第三方支付業者缺乏合適的驗證工具，且信用卡驗證支援 FIDO 仍在發展中，加上身分識別在電商用戶端和支付端整合不易所造成。所幸，基於以下理由仍看到改變契機：1. 政府積極推廣 FIDO 並建立相關作業指引；2. 以 TW FIDO 為典範，突破 FIDO 註冊前的驗證門檻；3. 透過服務規模化降低技術與成本門檻；4. 主管機關願意協助支付業者爭取驗證工具。在會中最後座談階段，主持人無店面零售商業同業公會秘書長許生忠引言：「登入」是駭客竊取數據最常借道的破口。

文化部資訊處處長莊舜清接棒：有鑑於 80% 資料外洩都是肇因於弱密碼設置，幾經思量，導入 FIDO 是最好選擇。甫經修正的「內政部行動自然人憑證系統介接申請要點」已將該系統的服務對象擴大至適用個人資料保護法之公務機關或非公務機關，並以行動自然人憑證作為網路中之身分識、數位簽章及加解密用途，一般民眾只要手機


照片人物：藍新科技產品規劃處處長林承勳

下載應用程式 (APP)、連線至系統平台完成認證後，這支手機就能成為身分憑證。藍新科技副總經理李偉琪就第三方支付業者立場提到，如何借助 FIDO 為買、賣雙方打造「防詐」的交易環境是值得深思的議題。

FIDO 聯盟台灣分會會長暨神盾公司副總經理張心玲介紹，FIDO 聯盟成立於 2013 年，迄今全球有逾 300 個會員、認證產品 (FIDO Certified Products) 已突破千項。FIDO 是很好的生態系，組成非常多元，參與其中有助於了解諸多國際標準並與國際龍頭廠商結緣；據 Yahoo! Japan 統計，導入 FIDO 後可降低 25% 的客服成本、使顧客上線購物時間增加 2.6 倍，而使用 FIDO 上線的消費者更高達 74% ！露天市集技術處協理陳贊元總結，做資安就像在買保險，做得越多、風控就越周全；惟考慮到並非所有裝置都支援 FIDO，採用分段實施將是較理想方式。