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

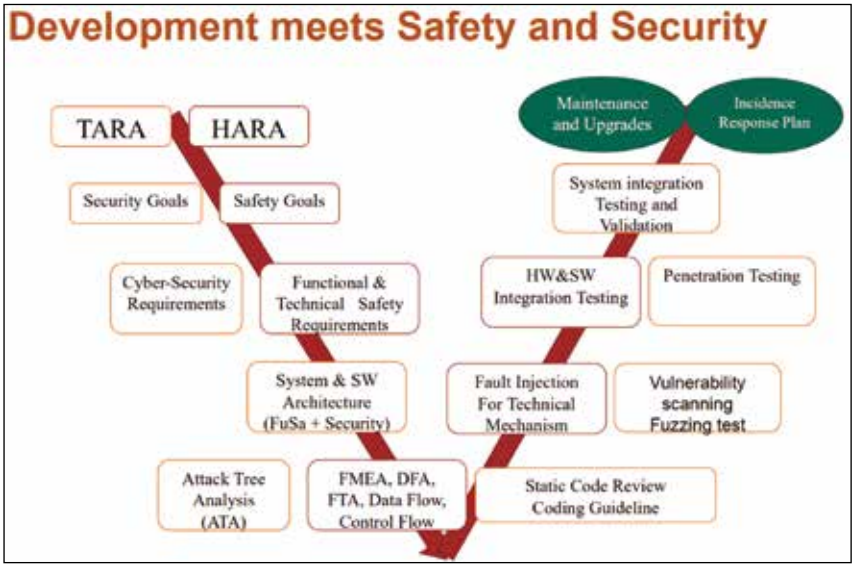
汽車趨向智慧化，自然而然亦成為資安重點防禦範疇。SGS 功能安全暨資通安全服務中心技術經理及功能安全專家張國樑表示，由於客戶端拉動，汽車電子廠商不得不日益重視信賴性 (Dependability) 等國際標準，業界期盼有一套「多合一」的方法分析與共通的開發流程以應對上述要求，並融入企業文化中。以此為前提，下有六大支柱：功能、效能 (可用性)、可靠 (耐用)、功能性安全、網路安全及預期機能安全 (SOTIF)，需要 IEEE 標準支援技術開發，為產品的設計驗證提供框架。

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。

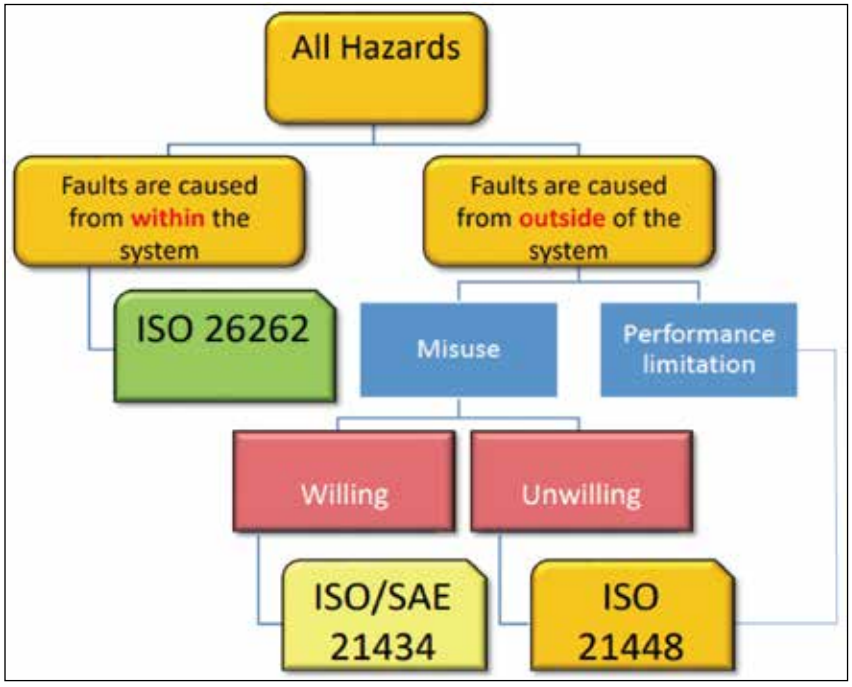
張國樑建議，廠商若同時要符合兩種規範，可在功能安全文件就緒後，就技術層面和系統級別推導出基礎系統架構，分析、評估是否存在資訊安全的威脅 (Threat Analysis and Risk Assessment, TARA)，進而推導網路安全要求。從系統觀來看資安的軟體層級，識別出網路安全的要求後，就能清楚掌握細部規範，例如，傳統通訊網路會要求晶片上要有控制器區域網路 (CAN Bus)，那麼，軟體如何編寫通訊協定與電子控制器 (ECU) 溝通？以及 CAN 規定須做加、解密以確保資料的完整性，要如何儲存、處理數據？加、解密要複雜到何種程度，採對稱型或不對稱型？

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。

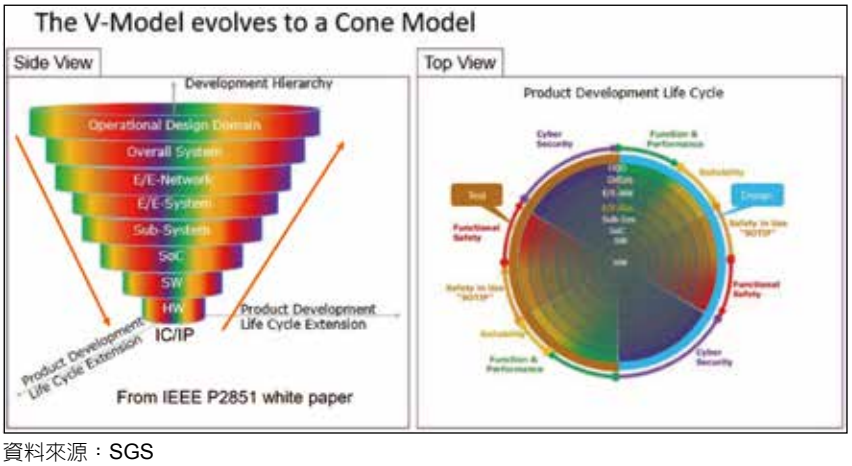
之後的測試方法與深度，亦是工程師最大的挑戰，從軟體網路安全需求、設計到導入須具備「可追溯性」。新近問世的 ISO21448 (SOTIF) 亦是 ISO 26262 的延伸，著眼於意外誤用、感測器／致動器／演算法性能極限等外部故障；簡言之，26262 關注的是系統失效，SOTIF 側重系統弱點。供應鏈的數據交換模式也因為須融合、共同統整規劃，從傳統的 V 字型視角 (V-Model) 轉為立體的圖錐形視圖

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++。

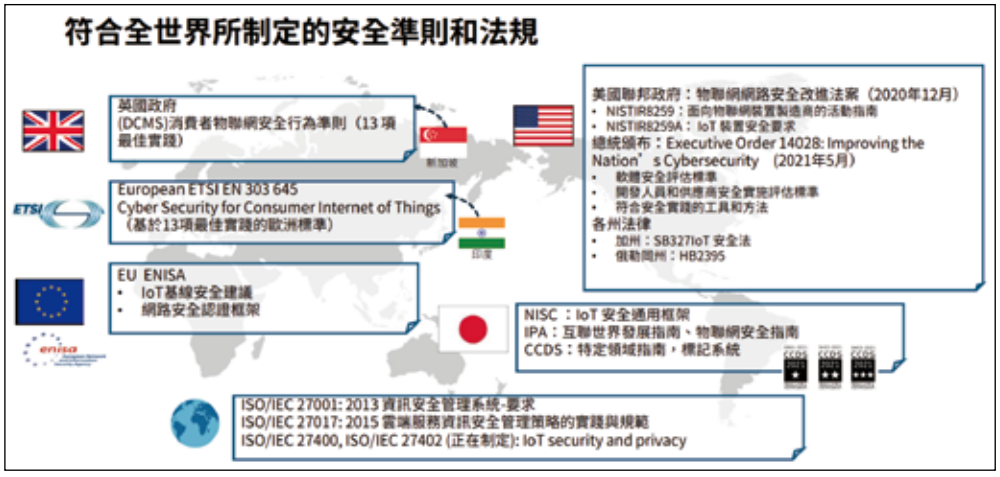
蔡本中表示，汽車開發對於開發工具的品質極其重視，使用靜態分析工具 C-STAT 不僅可掃瞄程式碼是否合規、設定編碼規範找出潛在隱患，還能明確指出哪一個 .c 檔的哪一行程式碼有誤，開發者可透過詳盡的說明文件了解程式碼規範，並有程式範例可供參考，另提供命令列模式可輕鬆整合 CI/CD。另一方面，對於變數初始化、字串和指標的使用需更加謹慎，以免造成安全漏洞，而 CERT 規範可檢查程式碼以增加安全性。此外，使用動態分析工具 C-RUN 可查找運行時才會發生的問題。

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