

控制器資訊安全驗證服務採購需求

一 採購標的與目的

本案辦理控制器資訊安全驗證服務，針對甲方指定之控制器、韌體版本及通訊介面執行威脅分析與風險評估 TARA、模糊測試 Fuzzing、滲透測試 PT，以及弱點整理與必要複測。測試應於甲方授權之隔離環境內進行，成果以測試範圍明確、證據可追溯、主要案例可重複執行及改善建議具可行性為原則。本案不以確認無任何弱點、取得產品認證或提供法規符合性證明作為驗收條件。

二 測試服務內容

測試範圍與執行規則

廠商應在測試前確認待測版本、資產、CAN 或 CAN FD、UDS、Ethernet 及其他實際開放介面，並提出測試計畫與 Rules of Engagement。內容應列明允許的工具、帳號與權限、測試時段、停止條件、備份或復原方式，以及測試資料的保存與交付方式。可能造成設備損壞或服務中斷的操作，須先取得甲方書面同意。

TARA 威脅分析與風險評估

廠商應參考 ISO/SAE 21434 的風險管理概念，依系統架構及介面資料建立資產清單、損害情境、威脅情境與可能攻擊路徑，評估影響與攻擊可行性，形成風險等級、資安目標、建議控制措施及殘餘風險。成果至少涵蓋 8 項代表性威脅情境；若主要資產不足 8 項，得以雙方確認的全部主要資產為準。

Fuzzing 模糊測試

廠商應就實際存在之 CAN 或 CAN FD 訊框、UDS 診斷服務及 Ethernet 或 IP 服務選取至少 3 個測試目標；若可測介面少於 3 個，則以全部可測介面為準。每個目標至少建立一組可重複執行之測試工作，涵蓋邊界值、異常長度、錯誤順序、非預期狀態或合理速率變化，並保存種子或 Corpus、組態、執行紀錄，以及 Crash、Hang、Reset 或異常回應摘要。

PT 滲透測試

廠商應採黑箱或灰箱方式執行至少 5 項代表性案例，可包含通訊服務盤點、身分驗證與權限控制、UDS 診斷存取、韌體更新或回復機制、除錯與管理介面、網路服務設定及敏感資訊保護。每項案例應記錄前置條件、測試步驟、實際結果、影響、證據及改善建議。未經同意不得執行破壞性利用或將測試流量送至非本案系統。

三 交付內容

項次	交付項目	最低內容
1	測試計畫與執行規則	測試範圍、版本、介面、時程、工具、權限、停止條件及復原方式
2	TARA 文件	資產、損害與威脅情境、攻擊路徑、風險評估、資安目標、控制措施及殘餘風險
3	Fuzzing 測試專案	Harness 或測試程式、種子或 Corpus、組態、執行方式及異常紀錄
4	PT 測試資料	可交付的測試代碼、命令或步驟、必要證據與重現條件
5	弱點與改善清單	弱點說明、影響介面、風險分級、證據、改善建議及複測狀態
6	測試工具與報告	工具及版本清單、操作說明、完整測試結果、限制、結論及管理摘要

四 驗收方式

驗收項目	通過條件	佐證
範圍與證據	測試版本、介面、工具及執行規則均有紀錄，測試證據可對應交付報告	文件檢點
TARA	至少 8 項或全部主要資產完成分析，風險、控制措施及殘餘風險可追溯	TARA 文件
Fuzzing	至少 3 個或全部可測介面各完成一組工作，可依操作說明重複執行並產生執行摘要	紀錄與現場執行
PT	至少 5 項案例完成執行，均有結果、風險分級、證據及改善建議	PT 測試報告
移交與複測	甲方人員可重複執行 1 組 Fuzzing 工作；履約期間如提供修正版，重大或高風險項目得執行 1 次複測	操作與複測紀錄

五 配合事項及範圍邊界

- 甲方提供待測控制器、指定韌體、架構與介面資料、DBC 或 ODX、必要帳號或金鑰，以及可復原的測試環境。廠商不得在交付資料中保存未經同意的憑證或機密。
- 本案不含生產環境攻擊、社交工程、第三方雲端或外部系統測試、實體破壞、長時間阻斷服務、原始碼全面稽核、ISO/SAE 21434 認證或 UNECE 法規符合性證明。
- 弱點之發現本身不構成驗收不合格。驗收應以約定測試是否完成、證據與風險說明是否完整，以及成果是否依規定交付為判定基礎；工具如有額外授權或相容性限制，須於履約前揭露。