經濟部 108 年度
自動駕駛感知次系統攻堅計畫
合作研究計畫

《自駕車資訊安全監控與研究》
建議書徵求文件

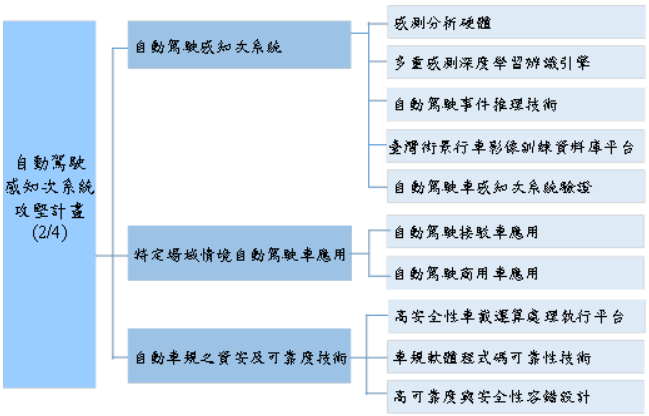
財團法人資訊工業策進會

中華民國　108　年　2　月　15　日

108年度合作研究計畫建議書徵求文件

一、 簡介

為執行『自動駕駛感知次系統攻堅計畫』中之『自動車規之資安及可靠度技術』--『高安全性車載運算處理執行平台』部分，其中包含建立『多層次資訊安全監控技術』，基於國際自動駕駛發展趨勢與我國資通訊產業優勢及缺口，發展自動駕駛感知次系統與相關技術，建立車規等級資安與驗證能量，以建構國內自動駕駛車產業鏈，規劃連結2大目標市場：將自動駕駛感知次系統導入泛用車輛整車國際展示；及將首套特定場域自動駕駛車接駁服務系統聯結車廠，導入國內場域示範運行；母計畫架構如下圖：



其中母計畫所開發之『高安全性車載運算處理執行平台』中之『多層次資訊安全監控技術』，可促進臺灣資安相關產業、安控產業、網路產業升級，強化資安防禦技術與能力，協助汽車電子供應商導入自動化駕駛供應鏈。

二、 計畫目標

根據母計畫所研發之『多層次資訊安全監控技術』建構CAN(Controller Area Network)之資訊威脅監控技術及規劃導入對虛擬化執行環境之檢測支援，同時強化對檢測模組的自我保護能力，確保檢測過程之可靠性。透過與車載機業者開發之多層次資訊安全閘道器，收集車輛上之CAN網路資訊，建立自動駕駛車後台ECU資訊監控平台，推展具備資訊安全監控機制之車載系統。

三、 計畫範圍

1. 藉由客製化信號介入硬體模組，透過車輛之標準 CAN 網路介面，解析並監控 CAN 網路上之各項 ECU。另一方面，客製化信號介入硬體模組可接收第三方設備(如 PC、車載機或遠端平台)發送 CAN 網路干擾資訊，如 Flooding Attack、Fuzzing Attack、Targeted Probing 等，觀測 CAN 網路與 ECU 等動作行為，建立威脅模型。
2. 透過實際部署客製化信號介入硬體模組至不同車款上，於車輛行進中蒐集 CAN 網路資訊，建立 CAN 網路運作標準模型，累積比對參照所需之資料。

四、 預期成果(明確說明合作研究成果之產出)

- 蒐集解析 5 款以上(Mitsubishi、TOYOTA、Mazda、Ford、Nissan、Lexus、Audi…等)不同品牌車系 CAN 網路資訊（CAN-ID 與 CAN Message），提供更完整的車身數據。
- 開發自動駕駛車後台 ECU 資訊威脅監控技術，針對至少 5 項威脅進行監控。
- 將研究方法與實驗觀察結果做整理，以技術文件與研究報告呈現。

※前述成果如有專利構想或專利申請產出時，需注意專利申請之新穎性(novelty)。因凡經公開發表之研發成果，如擬申請專利，須於公開發表後 6 個月內完成，前述成果如是以論文方式公開發表，將無法取得大陸與歐盟等國之專利。*(※文字請保留，此括號文字請於正式版時刪除)*

五、 執行方式(包括計畫時程、計畫分工方式)

由本會提供細部規格、參考資料與開發環境設定，執行單位自行研究設計技術內容與實作。執行單位必須自行驗證其成果符合本委託計畫之需求。

計畫執行期間執行單位必須每月需召開至少一次會議，以瞭解執行進度與狀況。

六、 計畫期程及預估計畫總經費

計畫執行區間：108年01月01日 至 108年12月15日

總經費：700,000元

- 期中報告交付(ECU 資訊威脅監控成果報告)
- 技術報告交付(含 ECU 資訊威脅監控技術內容、測試與驗證方式)
- 系統安裝執行檔交付(含原始程式碼，說明文件與教育訓練)
- 期末報告交付(含彙整結果、研究結果、實驗結果與教育訓練)

七、 驗收標準(含教育訓練)

1. 技術報告
   - 技術模組使用說明文件。
   - 期中報告。
   - 期末報告(含彙整結果、研究結果、實驗結果)。
2. 程式原始碼
   - 包含技術報告中所定義之『ECU 資訊威脅監控技術』相對應之程式原始碼。並分別以個別獨立檔案區隔。
   - 以 C 或 C#語言撰寫。
   - 需有足夠之程式註解。
   - 提供 C 或 C# DOC 參考文件。
3. 功能測試
   - 所交付之 ECU 資訊威脅監控技術，檢視是否符合項目相關監控之要求。
4. 專業論文一篇

八、 技術能力需求(請詳述所需要之技術能力或專長)

- 熟悉 CAN Bus 網路技術
- 熟悉車輛監控技術

附件1：契約書格式

1-1：計畫書格式

1-2：經費動支報表

1-3：成果報告撰寫須知

1-4：報告格式

1-5：論文格式

1-6：保密聲明書

1-7：委託匯款同意書