經濟部107年度

《自動駕駛感知次系統攻堅計畫（1/4)》

合作研究計畫

# 《自駕車多層次資訊安全監控技術》

# 建議書徵求文件

財團法人資訊工業策進會

中華民國 107 年 3 月 16 日

# 107年度合作研究計畫建議書徵求文件

## 一、簡介

近年來發展自動駕駛技術為國際主流趨勢，根據CB Insights研究指出，隨著無人駕駛車的熱潮持續延燒，除了傳統汽車大廠投入研發之外，矽谷為主的Apple、Google、Tesla、甚至Uber也正在發起研發自動駕駛車的戰爭，目前全球有高達30家公司投入無人駕駛車研發的行列。

自動駕駛是因演算法、軟體得以而起的汽車革命，國內資通訊、晶片、車用電子、車用設備等產業供應鏈完備，若能補足軟體及軟硬體整合能力，加上台灣產業的彈性與成本控制能力，有機會因應自動駕駛大趨勢，發展具國際競爭力的產品。其中，在自駕車規之資安及可靠度技術方面，發展車用Cyber Security資訊安全核心通常包括以下：車載安全執行平台、車規軟體開發輔助驗證工具、可靠度弱點檢測與功能安全設計合成工具，符合MISRA-C、ISO 26262、SAE J3061等車規安全設計流程；而自駕車服務的網路控制能力，為傳統車載平台也帶來了全新的安全挑戰課題。

在自動駕駛的應用過程，經由網路連線控制後，使得車載系統遭受駭客攻擊的潛在安全影響層面無限擴大，因而即便面臨與一般資訊系統相當的網際攻擊資安威脅，卻更易成為被駭客鎖定之重大攻擊目標。此外，不論如何堅強的防衛仍不免面臨到潛在系統管理安全及未知軟體漏洞威脅，未來自駕車或無人載具運算處理執行平台的設計，相較於一般資安防護系統，更需強調如何在駭客入侵後仍能確保系統維持安全運作，以爭取足夠時間發現並修正漏洞或安全管理缺失。

因此，在發展自駕車智慧引擎核心的安全車載運算處理執行平台時，重要的核心設計需考量確保惡意程式無論以何種方式侵入系統均不能被執行起來；多層次安全網路架構，以控制隔離入侵損害範圍，並爭取異常偵測診斷與進行後續更新修正之時間。讓自駕車在面臨各種網際攻擊，造成部分系統失效或無法控制時，仍可切換至安全復原模式，以維持系統安全運作，並等待威脅排除。

## 二、計畫目標

考量資安系統的保密性與私有性，建立車身網路與車輛聯網之隔離層，使平台形成多層次架構亦是重要議題，透過多層次安全網路架構，以控制隔離入侵損害範圍，並爭取異常偵測診斷與進行後續更新修正之時間，以達到對假冒之數據遙控訊號穿透至車身控制網路進行防護。

## 三、計畫範圍

基於資安保護的考量，目前實作方式並無明確標準與規範，故本計畫欲發展符合自駕車需求規格之資訊監控技術，研究自駕車資安需求特性，發展專屬之多層次資安監控與相關系統，提供外部監控模組針對聯網資訊與車身資訊交換狀況進行監控之技術與規劃，以利未來導入既有商業化資訊安全架構至母系統。

## 四、 預期成果

針對發展符合自駕車需求規格之資訊監控技術，參照國內外相關的資安監控應用及標準規範，將研究方法與文件蒐集結果做整理，以技術文件或研究報告呈現，提出一套完善之資安監控技術規劃，作為發展多層次資安監控與相關系統的參考與依據。

※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。

## 五、 執行方式

計畫執行期間執行單位需於期中期末召開至少各一次會議，以利甲方瞭解執行進度與狀況。甲方可提供相關參考資料，由執行單位進行研究設計其技術內容與規劃，透過技術文件或研究報告方式呈現，使其成果需符合本委託計畫之需求。

## 六、 計畫期程及預估計畫總經費

計畫執行區間：107年01月01日至107年11月15日

總經費：800,000元

- 107年07月15日期中技術文件交付(含自駕車需求規格之資訊監控技術架構規劃)
- 107年10月30日期末報告交付(含期中技術文件所定義之資訊監控技術架構與規範、自駕車資安需求特性等)

## 七、 驗收標準(含教育訓練)

甲方得依需求規格書所定項目及階段辦理驗收，乙方依契約規定應履行服務工作之責任。

1. 技術報告
   - 期中技術文件一份
   - 期末報告一份
2. 工作會議
   - 期中工作會議一場
   - 期末工作會議一場

## 八、 技術能力需求

- 熟悉資安領域之相關技術(如:系統防禦技術、資安系統監控、資安弱點評估及防護、通訊網路安全技術等)
- 具備資安相關技術開發經驗與應用實績(如:資安防護身份認證系統建置、車聯網相關資安整合應用、跨平台之資安應用等)

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