2013 台北國際自動化工業大展與機器人展

產學合作成果發表

專案 / 研究主題　**基於仿真設計平台開發高度安全性系統之安全流程**

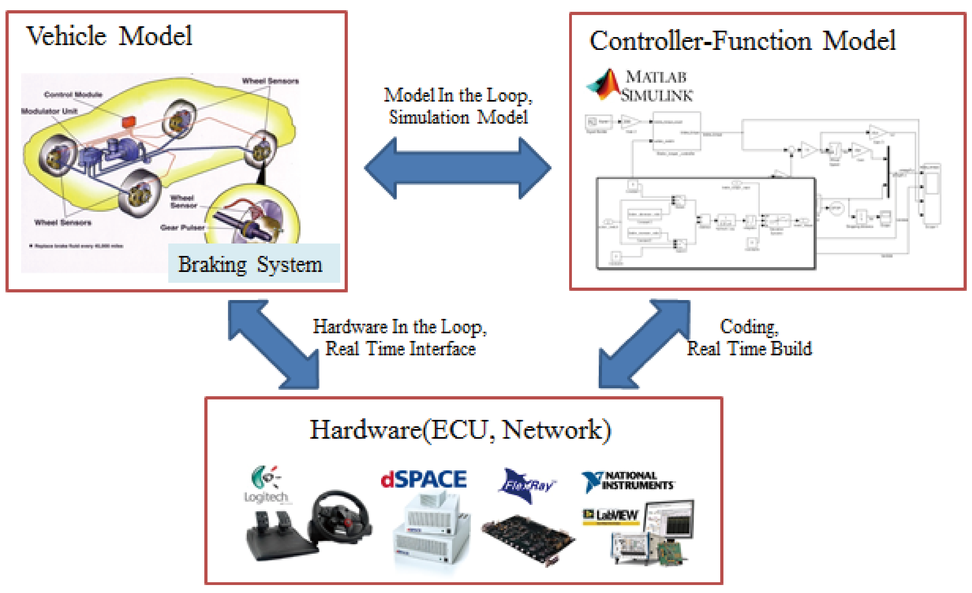
學 校 系 所： 國立台北大學 - 電機工程學系 智慧車電系統實驗室

計畫主持人： 陳永源 教授

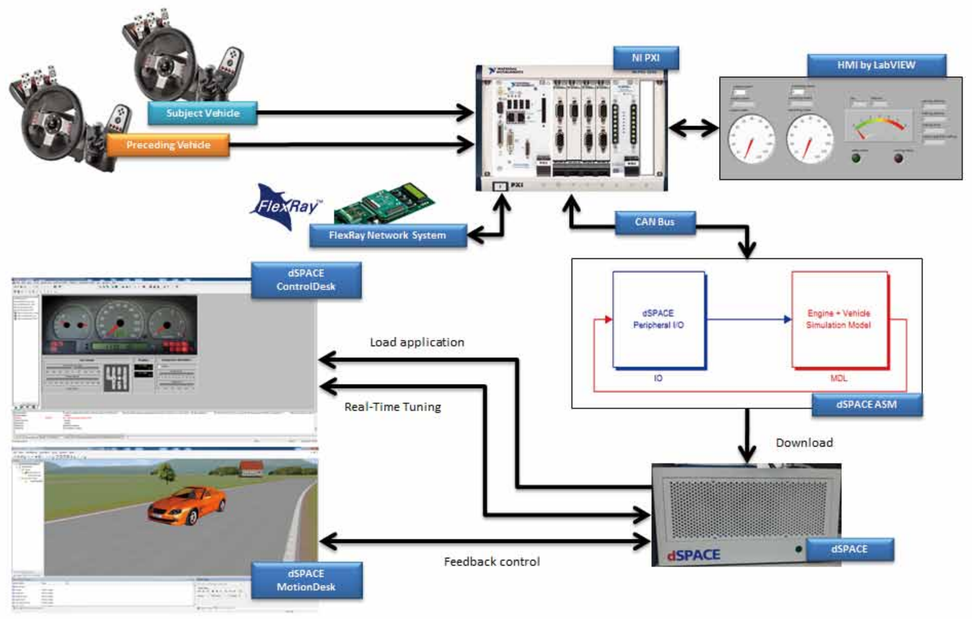
計 畫 重 點： 在本計畫中，我們將針對分散式線傳控制系統，導入國際功能安全規範 ISO 26262，研究其安全性 / 可靠度之相關議題，包括提出有效的系統化安全設計 / 驗證程序和開發平台，以及研發有效的容錯機制和錯誤注入、模擬分析環境。有關容錯機制，我們將開發適用於分散式線傳控制系統容錯機制，並有效地整合了各種不同的設計方針，以達到更全面性的分散式線傳控制系統容錯設計。我們將設計一個線傳緊急煞車控制系統模型，並透過強化容錯機制來增強其強韌度，降低危害所造成的風險傷害，並且透過預估模型或是錯誤模擬環境，來分析不同容錯機制對於系統整體可靠度之影響，試找出在可靠度提升以及額外硬體成本與效能下降間之平衡點。本計畫之核心價值，是希望提出一個導入國際功能安全規範於分散式線傳控制系統之容錯設計與驗證流程，讓設計者可以從系統規格需求開始，定義功能安全等級來發展安全目標，進而利用容錯設計與驗證流程，來設計開發系統功能，並符合國際功能安全規範之要求。

效益 / 特色： 隨著分散式線傳控制系統逐漸成為汽車電子系統中的主流，在開發高度安全性相關的汽車電子系統的過程中，系統的安全性與強韌度的問題必須得到解決。這是分散式線傳控制系統主要面臨的問題與挑戰。因此，應該提出有效的安全設計和驗證方法，以幫助降低複雜的設計與驗證過程。本論文針對高安全性系統如何導入國際功能安全規範 ISO 26262 安全設計與驗證程序，提出在模型化基礎設計平台中有效率的系統化安全設計 / 驗證與風險降低流程 (SVRR)。以個案研究的方式，利用 National Instruments PXI 與 dSPACE 建立系統設計與驗證平台並且開發一套煞車系統。故障注入基於模型的實驗結果表明，該系統組件的故障對於系統嚴重程度和系統的強韌度，然後，採用容錯機制以保護最脆弱的部件，提高了系統的安全性 / 強韌度。分析容錯機制對於系統整體強韌度 / 安全性的影響。

教 授 專 長： 容錯系統設計與分析、車用電子系統設計與開發、線傳駕駛控制系統設計與驗證、可靠度工程、系統機制安全設計與驗證。



〔圖一〕系統模型化設計流程



〔圖二〕車電線傳系統設計驗證平台