經濟部 110 年度
《臺灣資安卓越深耕-半導體及資通訊供應鏈
資安關鍵技術發展計畫》
合作研究計畫

《晶片軟體設計管控流程計畫》

建議書徵求文件

財團法人資訊工業策進會

中華民國 110 年 3 月

110 年度合作研究計畫建議書徵求文件

一. 簡介

近年來陸續發生多起晶片漏洞與攻擊事件，如 CPU 的 Meltdown、Spectre、Foreshadow 等漏洞；FPGA 的 Starbleed 漏洞；DRAM 的 Rowhammer 攻擊等，影響使用 Qualcomm、Intel、AMD、IBM、ARM 等晶片之電腦、平板及手機設備。觀察目前發現的漏洞，幾乎都是因晶片設計缺陷而造成，由於晶片的設計與產製特性，要在發布後像軟體一樣以更新方式進行安全性修補幾乎不可能，因此更需要建立晶片軟體設計開發威脅建模及資安規範，以避免最終產品發生與資安相關的問題。

爰此，臺灣資安卓越深耕-半導體及資通訊供應鏈資安關鍵技術發展計畫 (以下簡稱主計畫)將延續 FY109 科發計畫之研發成果，完善安全軟體開發管理框架，並擴充與優化開發活動支援及資安檢測工具，強固晶片安全軟體開發品質，並與國內晶片設計業者持續合作，完備管理框架與晶片設計流程之一致性，規劃建立國內 IC 晶片軟體資安生態系統。

本合作研究計畫因應主計畫之目標，預計發展晶片安全軟體開發流程管控工具，重點研發威脅分析與風險評估工具，建置符合 IC 設計業者需求的晶片安全軟體開發管理平台，期能有效提升廠商安全軟體開發成熟度，使我國半導體產品品質保持世界級競爭優勢。

二. 計畫目標

本合作研究計畫目標為建置符合 IC 設計業者需求的晶片安全軟體開發管理平台，導入晶片設計廠商進行概念性驗證，及調查半導體產業產品生命週期與開發流程現況，並蒐集相關資安需求，作為主計畫建立 IC 晶片軟體安全開發框架之參考。

三. 計畫範圍

本計畫預期工作項目包括：

1. 晶片設計資安需求調查

   藉由半導體產業諮詢，產出半導體產業威脅建模及風險評估需求分析、供應商資安管理需求分析等報告。

2. 晶片安全軟體開發管理平台與概念性驗證

   整合各資安工具模組，完成晶片安全軟體開發管理平台，導入 3 家晶片設計廠商進行概念性驗證。

四. 預期成果

1. 完成 2 場產業諮詢會議，並產出半導體產業威脅建模及風險評估需求分析報告、半導體產業供應商資安管理需求分析報告。
2. 完成 3 家晶片設計廠商概念性驗證，並產出 1 份晶片設計場域實證導入成果報告，描述概念性驗證成果。

※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

本計畫運用業界的研發能量與領域智識，配合主計畫「臺灣資安卓越深耕-半導體及資通訊供應鏈資安關鍵技術發展計畫」提供晶片安全軟體開發管理平台各資安工具模組，進行如「計畫範圍」所定義分析與開發。

預計將結合業界之研發能量與領域實務面經驗，回饋給主計畫技術研發方向，透過雙方相互合作討論的方式來進行。本計畫亦需提供相關系統之教育訓練及經驗分享機制，藉此增進本會研究人員的專業能力，以提升本合作案成果之效益，相關執行方式步驟如下：

1. 辦理 2 場產業諮詢會議。
2. 完成晶片軟體設計流程管理系統。
3. 導入 3 家晶片設計廠商進行概念性驗證。

六. 計畫期程及預估計畫總經費

計畫執行區間： 110 年 5 月 1 日 至 110 年 12 月 15 日

總經費：1000,000 元（含稅）

七. 驗收標準

1. 110 年 8 月 15 日完成期中報告，內容應包含半導體產業威脅建模及風險評估需求分析報告、計畫進度報告等。
2. 110 年 12 月 15 日完成結案報告及開發文件。
3. 結案報告：內容應包含半導體產業威脅建模及風險評估需求分析報告、半導體產業供應商資安管理需求分析報告、晶片設計場域實證導入成果報告等。
4. 開發文件：內容應包含晶片軟體設計流程管理系統分析與設計文件、系統測試報告書、系統弱點掃描報告書、系統管理手冊、系統使用手冊。
5. 本專案製作完畢後，乙方需將系統移轉至正式機器上，並可執行運作；並能於指定環境建立 Demo Site。
6. 乙方須提供程式、資料庫原始碼，提供甲方留存。
7. 為建立團隊對於相關程式運作機制及操作之了解，提供教育訓練。
8. 進度討論會議：每二週至少召開一次進度研討會議。

八. 技術能力需求

本合作研究計畫執行人員須具備資訊領域相關基礎知識背景包含：

1. 平台開發及營運實證經驗。
2. 其他：如熟悉 OWASP Top Ten 攻擊手法或 BSIMM 等。