

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

《晶片安全規範研究計畫》  
建議書徵求文件

財團法人資訊工業策進會

中華民國 110 年 1 月 1 日

# 110年度合作研究計畫建議書徵求文件

## 一、 簡介

當今世界不論是國防軍事系統，或是與國民生計相關的關鍵基礎設施，都會用到電腦、電子設備、通訊等資通訊技術(以下簡稱ICT)，且對ICT依賴程度日漸增加。而在ICT採購全球化趨勢下，ICT產業供應鏈安全不僅與國家安全有關，也是所有產品與服務供應鏈的基礎。在ICT供應鏈中，各種軟硬體、應用程式、資訊服務，多少會使用外部供應商技術元件，但因為使用者可能無法有效掌握這些外部技術元件的安全性，或不確定供應商、合作夥伴環境的資安防護程度是否足夠，造成駭客攻擊一旦往產業供應鏈上游深入，將對供應鏈安全產生深遠的影響。

此外，IC晶片產品一旦發生資安問題，影響的層面包含消費者權益、營業損失、商譽受損、國際裁罰等。據此，本合作研究計畫從資安角度切入IC晶片產業，研擬晶片安全相關指引提供業界參考，以強化我國晶片產品資安體質。為達成上述目的，資策會執行經濟部「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」，欲委託學界協助完成晶片安全相關指引4份，目的是提供業者於產品設計研發製造過程中的資安控制項目及做法之參考。

## 二、 計畫目標

本計畫將對於晶片安全防護機制進行評估和研析，目標為研析如何以軟硬體防護技術來強化晶片產品從設計到實作層級之資安防護能力，過程中亦須思考如何從組織、程序、技術等各方面確保IC晶片安全，有條理地整理出4份晶片安全指引，包括：晶片安全強固指引、晶片安全設計指引、晶片安全設計最佳範例、晶片安全實現指引。

## 三、 計畫範圍

本計畫預計研究以下主要項目：

- 晶片安全強固指引：如何從多個構面增強晶片保護，包括晶片接腳、韌體保護等
- 晶片安全設計指引：在設計規劃階段(paper work)如何納入安全考量
- 晶片安全設計最佳範例：根據晶片安全設計指引，提供最佳範例
- 晶片安全實現指引：於FPGA階段安全之編程規定

## 四、 預期成果

本計畫須配合母計畫需要進行研究，並產出以下成果：

1. 於110年5月底交付2份草案如下：
  - a. 晶片安全強固指引草案
  - b. 晶片安全設計指引草案。
2. 於110年8月底交付2份草案如下：
  - a. 晶片安全設計最佳範例草案
  - b. 晶片安全實現指引草案。
3. 於110年11/20前交付4份完稿如下：
  - a. 晶片安全強固指引
  - b. 晶片安全設計指引
  - c. 晶片安全設計最佳範例
  - d. 晶片安全實現指引

上述指引內容至少須包含以下章節：

1. 前言(含目的、適用對象及章節架構)

2. ○○介紹(針對指引名稱○○，說明其重要性或相關的資安議題，例如曾發生的資安事件或理論上可行的弱點攻擊等)
3. 晶片安全○○指引(針對上述所提及的資安事件或弱點攻擊等之根因，提出防範機制或最佳範例)
4. 結論
5. 參考文獻
6. 附件(例如提供○○檢查表範例)

※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

- 合作計畫執行單位應配合本會計畫監控機制。
- 於計畫執行期間，合作計畫執行單位須配合計畫所需，每月至少固定一次與本單位進行研究心得報告與研討，報告內容以計畫範圍相關之技術主題為主。
- 於計畫執行期間，合作計畫執行單位須配合計畫所需，不定期與本單位回報研究進度與內容。

## 六、計畫期程及預估計畫總經費

計畫執行區間：110年4月1日至110年12月15日

總經費：800,000元

## 七、驗收標準(含教育訓練)

- 依本建議書徵求文件第四章「預期成果」規定，如期繳交相關成果。

## 八、技術能力需求

- 具IC電路設計或晶片硬體防護設計研究經驗，或擁有相關授課經驗之學界研究人員。
- 具備且熟悉硬體資安攻防之學界研究人員。
- 熟悉資安相關背景知識領域，並對系統攻防，弱點防禦，或惡意軟體等有實際操作或研究經驗的技術或學界研究人員。