我國半導體供應鏈資安推動現況

報告人：資策會資安所 蕭榮興 副主任

111年07月

scottie@iii.org.tw
02-66078924

關於資安所

定位

- 發展資安技術厚創新量能，以第三方協力角色建立人才、商模與資安認驗證制度，賦能產業轉型需求；並連結各方資源，創建多元資安聯防策略，以引導產業聯防生態運作與國際合作。

任務

- **發展資安智慧聯防生態**：切入產業資安缺口，結合資源共創生態；發展資安長好幫手服務，創建安全聯防。
- **推動實戰人才訓用合一**：結合場域訓用實證、搭配職能發展護照與人才市集平台，提供各產業資安實戰力人才訓用機制。
- **驗證技術產品資安合規**：接軌國際資安標準，建立第三方檢驗測技術及認驗證機制，推動產業資安，發展全球商機。

11年
政府機關
與業界服務經驗

200位+
領域資安專家

500家+
資安共創會員

資安所重點發展項目

What we own 資安所產品

5G資安解決方案

建立國內首套gNB、MEC、IoT Gateway 安全落實檢測技術

- 5G元件合規檢測、虛擬環境弱點掃描
- 5G核網攻防實證
- 異常流量偵測、DDoS攻擊減緩

IC晶片軟體資安

確保IC產業晶片軟體安全合規切入國際大廠供應鏈

- 晶片資安檢測工具UFO
- 建立安全軟體開發要求基準
- 協助導入BSIMM管理機制
- 建立半導體產業供應鏈的網路安全管理

IoT資安檢測

研發智慧型資安技術，發展IoT資安產業

- 物聯網設備檢測
- CMAS 行動App安全檢測
- 建置國際級檢測實驗室，建立IEC62433技術典範

共創資安平台

提供智慧製造與工控資安顧問服務，支援產業數位轉型

- 建置工控Testbed，推廣OT資安研訓
- ICTD 智慧製造資安防護
- 結合垂直領域資安應用，建立跨廠、跨域生態系

AI智慧型資安

建立國際情資聯盟，並推廣DevSecOps合作模型

- 主動式弱點發覺，進行情資萃取
- 惡意威脅偵測
- 資料隱私防護與去識別化

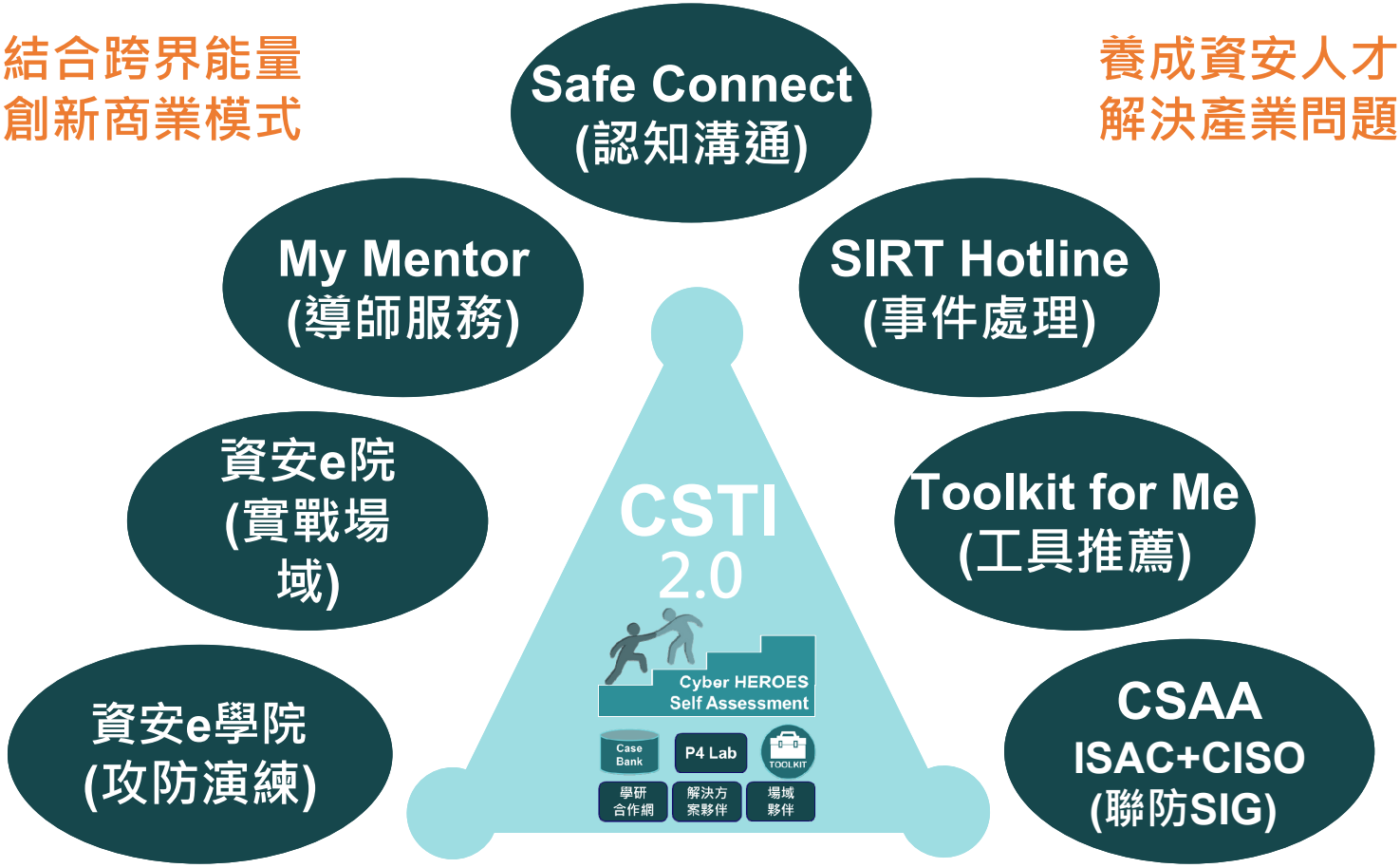
CSTI as a Service

What we have

資安所服務

結合跨界能量
創新商業模式

養成資安人才
解決產業問題



CSAA: Cyber Security Awareness Alliance

大綱

一、供應鏈資安國際發展趨勢

二、半導體產業在供應鏈安全之戰略重點

三、研發晶片惡意邏輯(硬體木馬)偵測技術

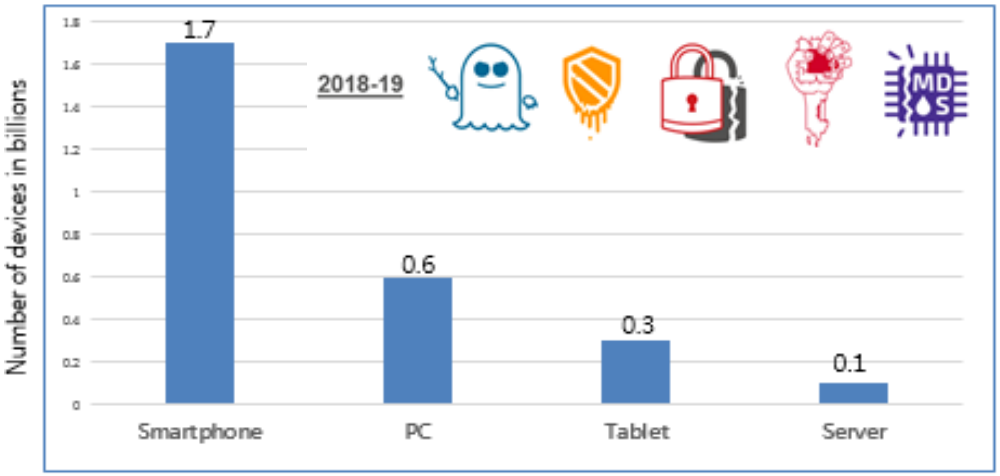
四、研擬晶片安全檢測規範

五、推動國內IC設計業者提升安全軟體成熟度

六、合作建議

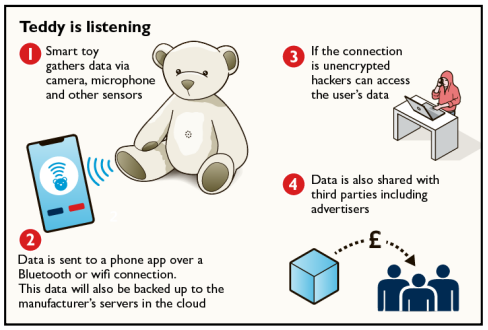
資安議題無所不在 從源頭即需防護

不僅處理器安全，只要有連網的設備，都面臨晶片安全問題

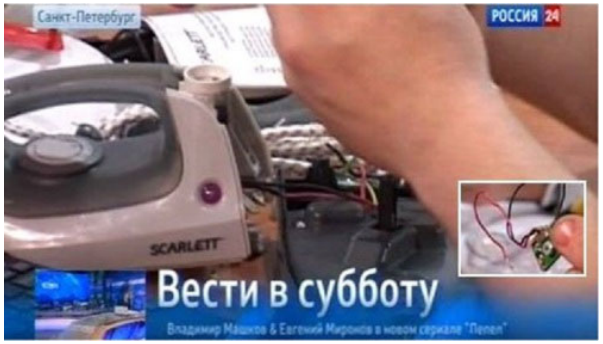


根據Statista 2018年統計處理器晶片漏洞，Meltdown and Spectre 引起易受攻擊的設備數量，智慧型手機數量高達17億

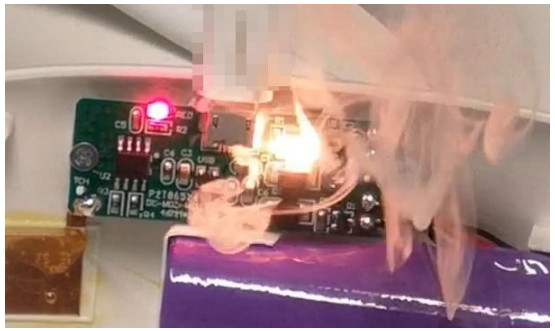
2019年高通的數位訊號處理器（Digital Signal Processor，DSP）含有重大的安全漏洞，約 10 億台 Android 裝置受威脅



透過微型藍芽或Wi-Fi天線，駭客能有效地與兒童說話和玩耍

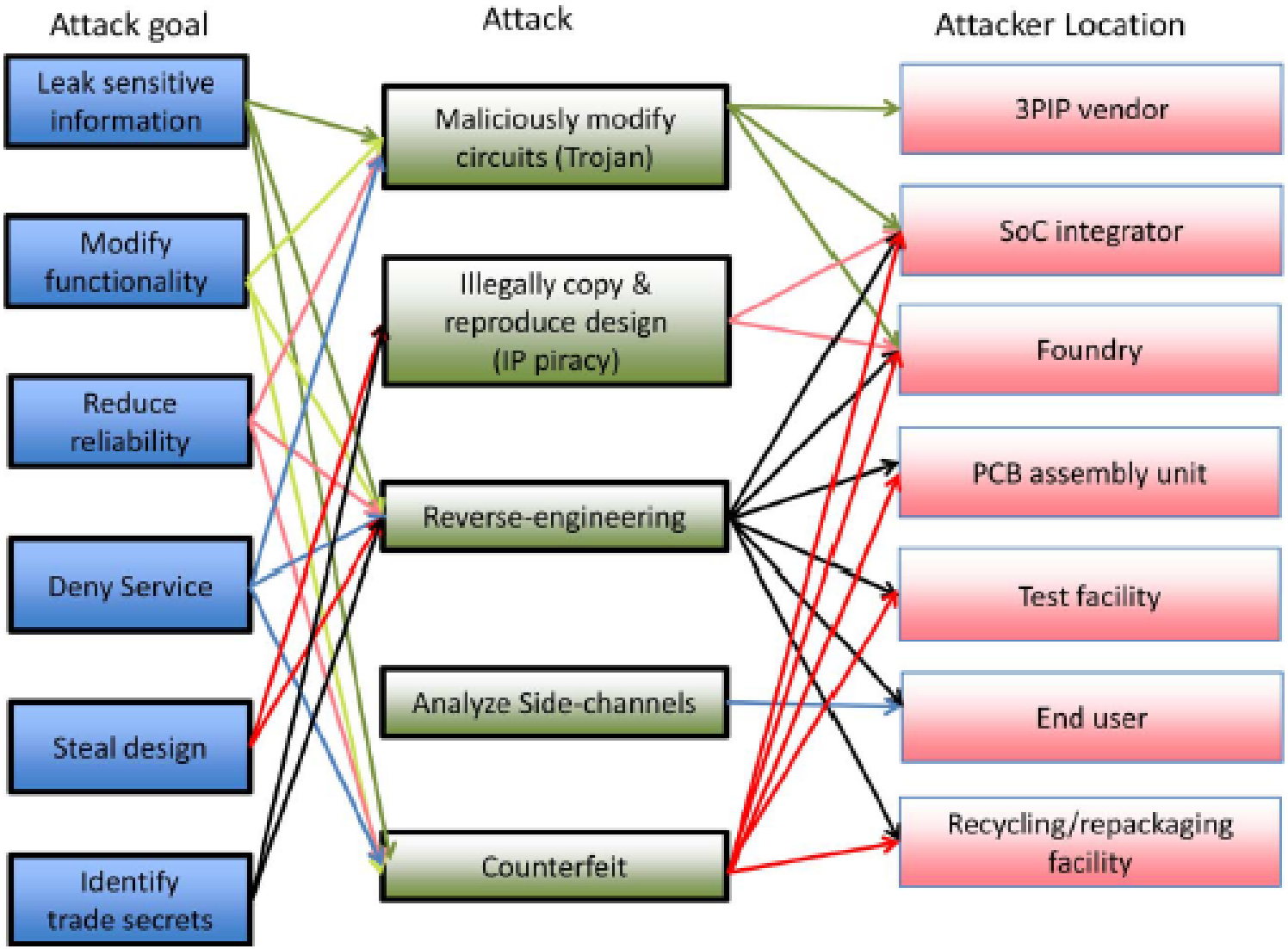


中國製造的家用電器包含間諜晶片，主要用於傳播病毒



充電設備遭BadPower攻擊時晶片燒毀情況

半導體供應鏈資安威脅



硬體供應鏈從資通訊上游-半導體供應鏈開始，晶片生產過程多由不同設計、製造及封裝測試公司進行，在整個IC晶片設計以及製造封裝測試過程中均有可能引入安全威脅

資料來源：Vol. 102, No. 8, August 2014 | Proceedings of the IEEE

英特爾及Arm處理器Spectre變種

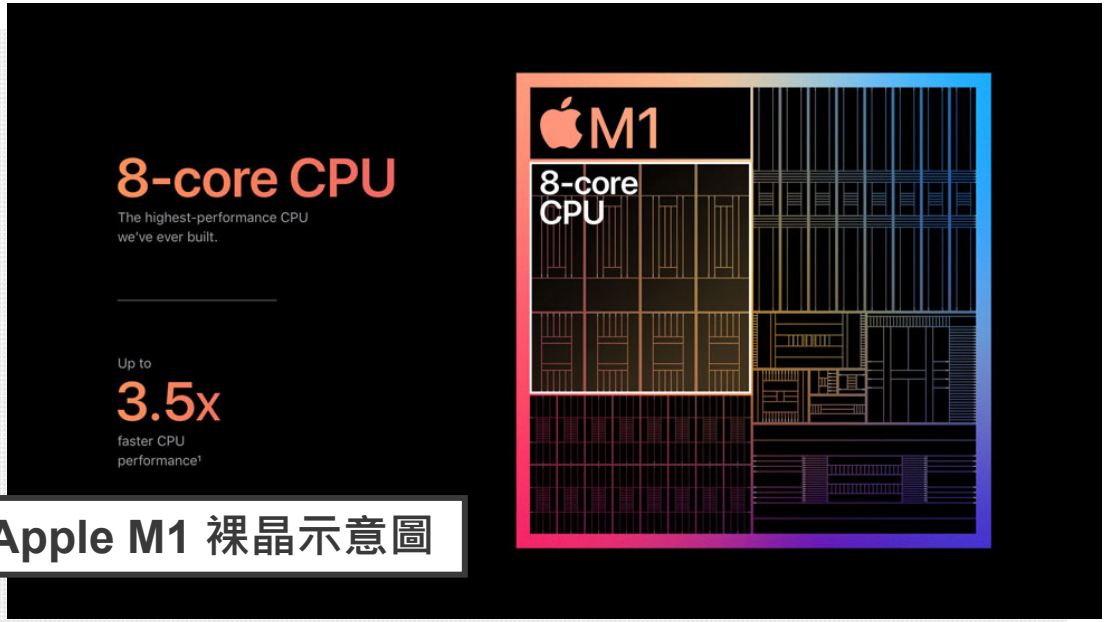
晶片設計資安風險

- 2022 年 3 月漏洞發布
- 漏洞編號：CVE-2022-0001~0002
- CVSS 評分：2.1 (低危害)
- 漏洞特性：
  - 機密性：部分衝擊
  - 完整性：無
  - 可用性：無
  - 存取複雜性：低
  - 驗證：不需要
  - 提權：無
- 在2018年曝光的CPU推測執行漏洞Spectre並沒有修補完全，該實驗室依然可透過其它管道開採其中的CVE-2017-5715漏洞，進而推測核心記憶體中的機密資訊
- 英特爾把所發現的漏洞拆分為CVE-2022-0001及CVE-2022-0002，而Arm對此僅提供一個漏洞編號CVE- 2022-23960，雙方皆已釋出安全建議

蘋果M1晶片漏洞

晶片設計資安風險

- 2022 年 6 月發現的漏洞
- 麻省理工學院 (MIT) 發現此漏洞
- 已向蘋果 (Apple) 提交漏洞，但尚未正式提交成 CVE 編號
- Apple 官方尚在理解漏洞問題
- 該漏洞可以：
  - 可竊取數據
  - 可完全控制系統
  - 可透過遠端運用
- 漏洞屬無法用軟體修補的硬體問題
- 其他安謀 (Arm) 架構晶片如高通 Qualcomm、三星 Samsung 等也可能有影響



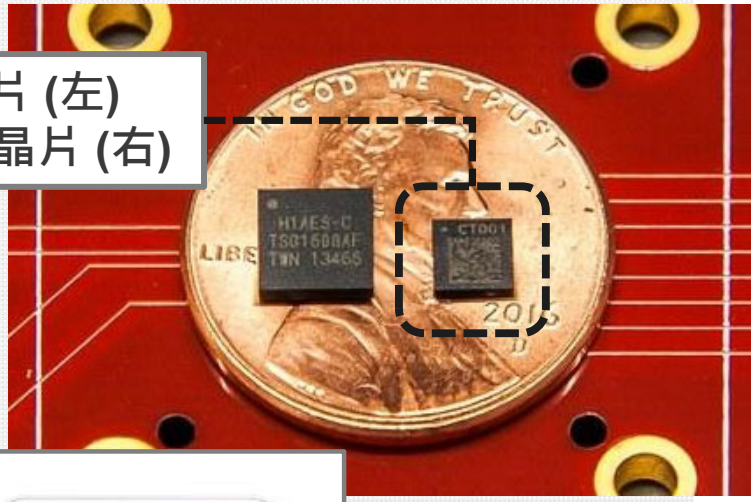
Apple M1 裸晶示意圖

圖片來源：Apple

谷歌Titan M晶片漏洞

晶片設計資安風險

- 2021 年 3 月漏洞發布
- 漏洞編號：CVE-2021-0452
- CVSS 評分：2.1 (低危害)
- Titan 晶片受影響：
  - 機密性：部分衝擊
  - 完整性：無
  - 可用性：無
  - 存取複雜性：低
  - 驗證：不需要
  - 提權：無
- 2019 年谷歌鼓勵入侵 Titan M 晶片，最高獎勵 100 萬美元
- 晶片本身的功能即在資安防護但卻出現漏洞，格外漏氣



圖片來源：Google

高通MSM系列晶片漏洞

產品資安合規

- 2021 年 6 月漏洞發布
- 漏洞編號：CVE-2020-11292
- CVSS 評分：7.2 (高危害)
- 資安業者 Check Point 發現此漏洞
- MSM 系列晶片受影響：
  - 機密性：完全衝擊
  - 完整性：完全衝擊
  - 可用性：完全衝擊
  - 存取複雜性：低
  - 驗證：不需要
  - 提權：無
- 多家品牌高階手機均受影響，包含谷歌、三星、樂金、小米、One Plus 等
- 波及全球約 30% 手機
- 駭客可存取手機簡訊或通話內容

MSM8916 晶片

MSM6246 晶片

谷歌 Pixel 4 智慧型手機使用高通 MSM 系列晶片

圖片來源：Qualcomm、Google

國內晶片產品漏洞

產品資安合規

- 2022 年 5 月漏洞發布
- 漏洞編號：CVE-2022-21743
- CVSS 評分：4.6 (中等危害的威脅)
- 溢出 (Overflow) 型漏洞
- 漏洞特性：
  - 機密性：部分衝擊
  - 完整性：部分衝擊
  - 可用性：部分衝擊
  - 存取複雜性：低
  - 驗證：不需要
  - 提權：無
- 共計 52 款晶片受影響，從 MT6580、MT8696 到 MT8797

迅鯤 (Kompanio) 1300T 為 5G、6 奈米晶片

Amazon FireTV 電視棒
使用 MT8696 晶片

圖片來源：MediaTek

國內晶片產品漏洞

產品資安合規

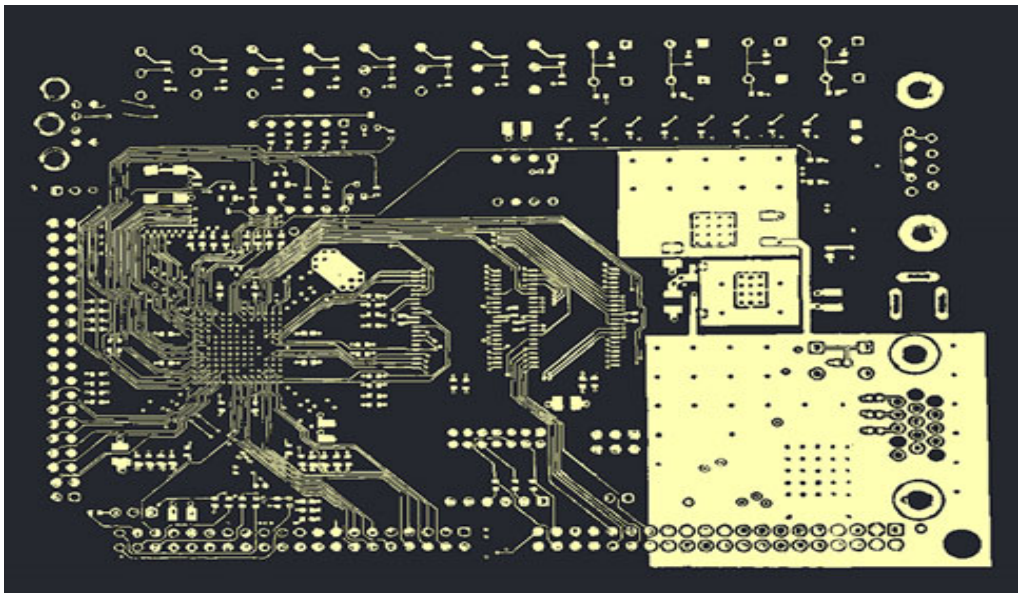
- 2021 年 8 月漏洞發布
- 漏洞編號：CVE-2021-35392/3/4/5
- CVSS 評分：7.8～10 (極高危害)
- 資安業者 IoT Inspector 發現此漏洞
- RTL8xxx 系列晶片受影響：
  - 機密性：完全衝擊
  - 完整性：完全衝擊
  - 可用性：完全衝擊
  - 存取複雜性：低
  - 驗證：不需要
  - 提權：無
- 約 65 家業者受影響，如 LG、ZyXEL、Netgear
- 近 200 多項產品受影響，如 IP 攝影機、Wi-Fi 路由器、Wi-Fi 強波器

RTL8198 晶片

使用 RTL8198 晶片的友訊 (D-Link) Wi-Fi 路由器 DIR-651

圖片來源：Realtek、D-Link

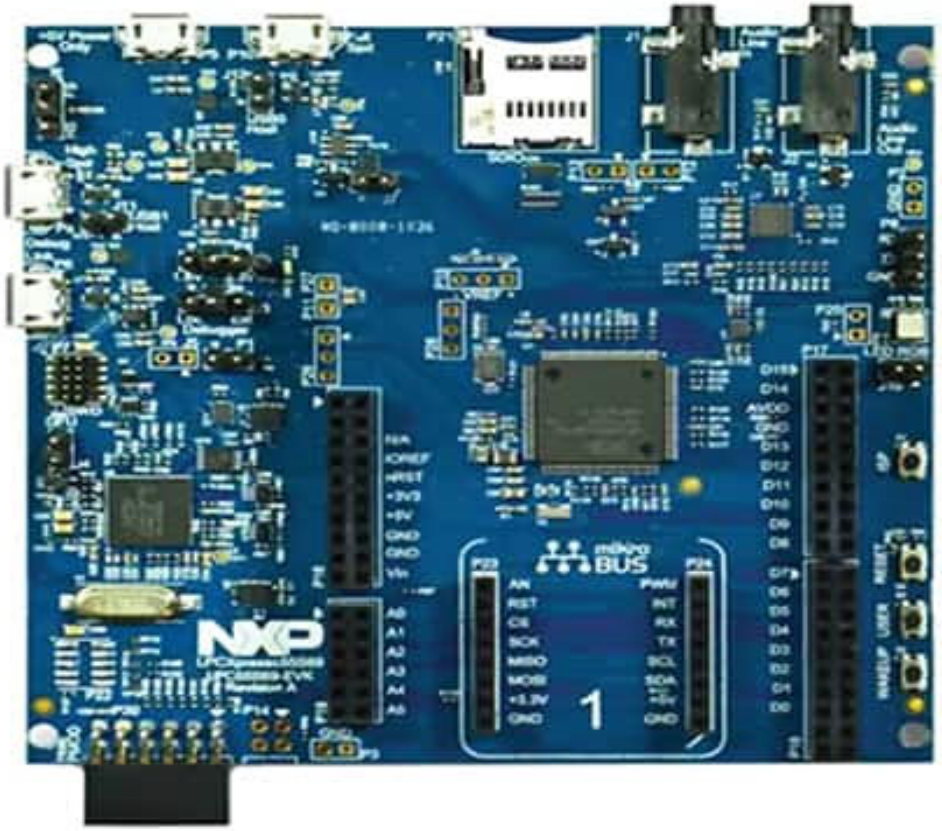
供應鏈成熟度風險



2018年10月《彭博商業周刊》（Bloomberg Businessweek）報導，包括蘋果和亞馬遜等近30家美國企業所採用Supermicro伺服器主機板，被中國間諜秘密植入不明晶片，通過破壞美國的技術供應鏈，從而使中國駭客得以深入探查這些網路。2020年彭博更進一步宣稱FPGA晶片廠商Altera安全長在某份報告中，承認見過會連線回中國的Supermicro晶片

2020年竹科至少有7家半導體相關公司被駭客攻擊，其中某家IC設計公司內網不但有駭客潛伏超過1年，其晶片產品設計圖等文件都被攻陷、閱覽。
最重大的證據，就是台灣受害者供應鏈被植入的惡意程式中，發現Winnti常用的特殊後門惡意程式「baseClient.exe」。中國挖不到就偷！7家竹科半導體廠遭駭從晶片設計到程式碼都要，在美國資安界引起很大轟動

晶片安全議題來自設計階段



硬體攻擊通常是由於半導體設計過程中未檢測到的漏洞或通過韌體造成的。這些攻擊可能發生在產品生命週期的各個階段，並可能導致晶片故障、拒絕服務或敏感資訊洩露。**硬體攻擊分為兩部分：**

- 故障注入等主動攻擊（導致IC故障和災難性系統故障）
- 旁道分析等被動攻擊（導致秘密資訊洩漏，例如-密碼的秘密金鑰）

半導體產業在供應鏈安全之戰略重點

近年資通訊供應鏈攻擊日益增加，尤其是硬體供應鏈攻擊更具破壞性。觀察國際半導體產業發展趨勢有三大資安樣態：

晶片設計資安

晶片設計過程中的**漏洞、後門**或通過**韌體**造成產品生命週期各個階段的硬體攻擊持續不斷。例如：2014威盛電子VT3421安全晶片「後門」事件

產品資安合規

因應國際**合規要求**，晶片產品必須**檢測通過如SESIP、IEC62443等國際安全標準**，確保所提供的晶片符合安全標準規範，向供應鏈其它廠商證明產品本身相關的資安漏洞已獲適當解決

供應鏈安全

供應鏈成員資安治理皆須達一定水準，各國也陸續增加**供應鏈安全政策要求(如美國國防供應鏈CMMC認證要求、歐盟汽車供應鏈ISO21434認證要求等)**，避免駭客集團從供應鏈上游取得商業機密資料，例如：2018台積電勒索攻擊、2020年竹科7家半導體公司晶片產品設計圖等被竊取

資安所研發與推動策略

晶片設計資安

- 缺乏自動化與系統化識別晶片安全漏洞檢測工具
- AI晶片應用易受對抗式攻擊，導致發生系統誤判或被破解

✓ **發展晶片惡意邏輯與旁通道攻擊檢測工具**，降低矽前、矽後階段維護修補之成本

✓ **研析AI模型攻擊檢測防護演算法**，降低機敏資料受汙染而對晶片之攻擊危害

產品資安檢測

- 外銷產品須事先取得國際檢測實驗室檢驗認證，才可外銷出口
- 多數業者不理解國際資安要求的內涵

✓ **成立通過SESIP認證國際晶片安全檢測實驗室**，協助晶片業者之晶片產品進行場域安全實證

✓ **建立半導體上、中、下游資訊安全快訊服務**，協助國內關鍵產業之企業產品合規

供應鏈成熟度

- 上游晶片產品出現資安問題，下游電子設備業者無法即時取得修復
- 國際大廠要求供應鏈廠商需符合國際資安標準或通過安全成熟度評鑑

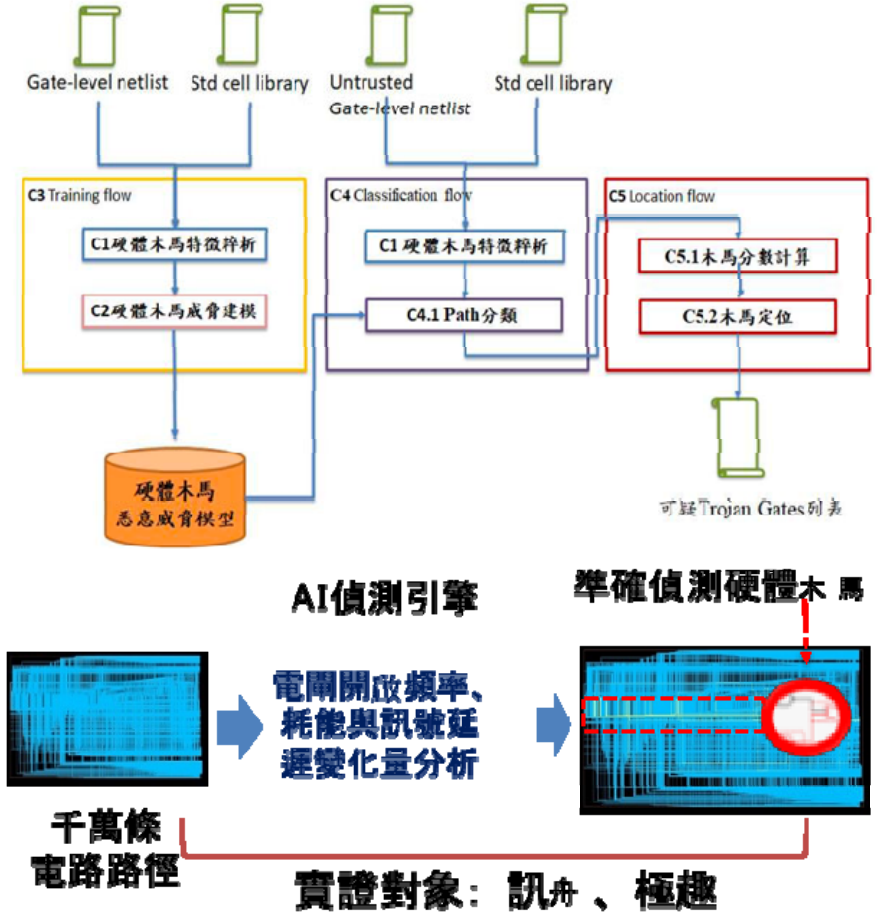
✓ 建構**晶片安全軟體開發管理框架**，研發各階段相對應之**安全活動支援工具**

✓ **提供半導體產業**導入安全軟體成熟度模型，輔導資安業者加入顧問及評鑑工作

研發晶片惡意邏輯(硬體木馬)偵測技術

領先全球晶片設計安全檢測，辨識木馬準確率達99%

- 與交大合作，藉由頻率、耗能、訊號延遲變化量特徵塑模，創新異常電路AI偵測引擎，準確率達99%，與國際知名研發機構(美國佛大) 水準並駕齊驅
- 協助工研院、擷O科技、中原大學等檢測110個晶片電路，包含RISC-V、8051單晶片微控制器之AES加解密電路、PCIe傳輸管控電路等，誤判率降低到10%以下(誤判率定義為廠商提供之無木馬樣本經由系統被誤判為帶有木馬之樣本的比率)。



論文發表：Impact of Cross-standard Cell Libraries on Machine Learning based Hardware Trojan Detection, In Proceedings of the 8th International Conference on Information Systems Security and Privacy - ICISSP, 420-425, 2022

惡意邏輯檢測技術推動成果

透過公協會合作、技術移轉、開源分享，促成產業檢測能量建立

研擬晶片安全檢測規範

- **晶片**是各種運算的核心，一旦發生資安問題，將直接影響上層**系統軟體**運作的安全性，因此催生本系列標準，用以涵蓋組成晶片產品的各層級元件資安要求
- 已和電電公會(TEEMA)合作，召集晶片業者、資安專家、資安檢測實驗室等，制定成為我國晶片產業資安標準，預計今年於GlobalPlatform國際會議上發布

第一部 晶片安全標準	規定晶片層的安全要求，包括執行核心運算的微控制器/微處理器，應在 1. 矽前(pre-silicon)階段避免晶片設計含有可疑電路 2. 矽後(post-silicon)階段應防範非侵入式的旁通道攻擊 3. 並規定了晶片封裝、韌體及除錯介面等相關安全要求 本標準適用於晶片廠商
第二部 系統軟體安全標準	規定了系統層及軟體層的安全要求，包括密碼安全、儲存安全、通訊安全等。 本標準適用於系統廠商及軟體廠商

建立晶片安全聯合檢測實驗室

- 透過策略同盟，於今年Q3成立「晶片安全聯合檢測實驗室」，從人力(領域專家)、物力(測試設備)、設施(實驗室)、商轉模式等，共構晶片安全檢測能量。
- 開始提供旁通道檢測(SCA)檢測服務，提供晶片設計業者，驗測其晶片安全性

晶片安全檢測測項

安全功能/非安全功能保護
- ☐ 基礎物理攻擊抵抗
- ☐ 進階物理攻擊抵抗

晶片本體
- ☐ TA測試
- ☐ SPA/SEMA測試
- ☐ DPA/DEMA測試

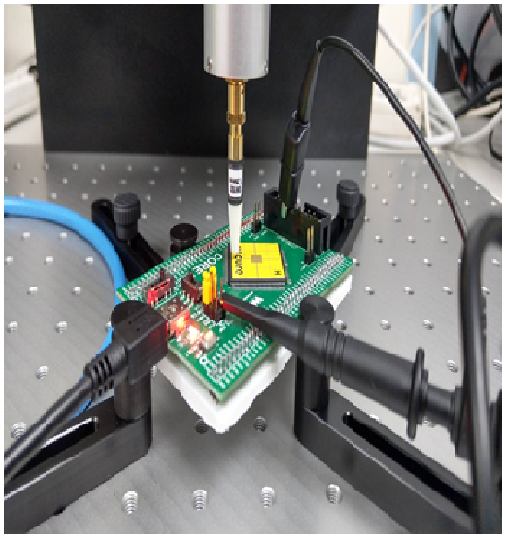
除錯介面安全
- ☐ 安全除錯保護
- ☐ 安全除錯身份驗證

封裝保護
- ☐ 晶片密碼模組通用保護
- ☐ 晶片密碼模組基礎保護
- ☐ 晶片密碼模組進階保護

韌體安全
- ☐ 機敏內容保護
- ☐ 可疑連結與程式碼檢測
- ☐ 韌體弱點檢測
- ☐ 韌體原始碼保護
- ☐ 韌體完整性保護

晶片設計
- ☐ 可疑電路測試

檢測實作



產業效益

- 可重複使用(reuse)已獲驗證的元件，減少重複測試的成本浪費
- 對購買已驗證元件的產品製造商，將受益於降低測試成本和縮短上市時間

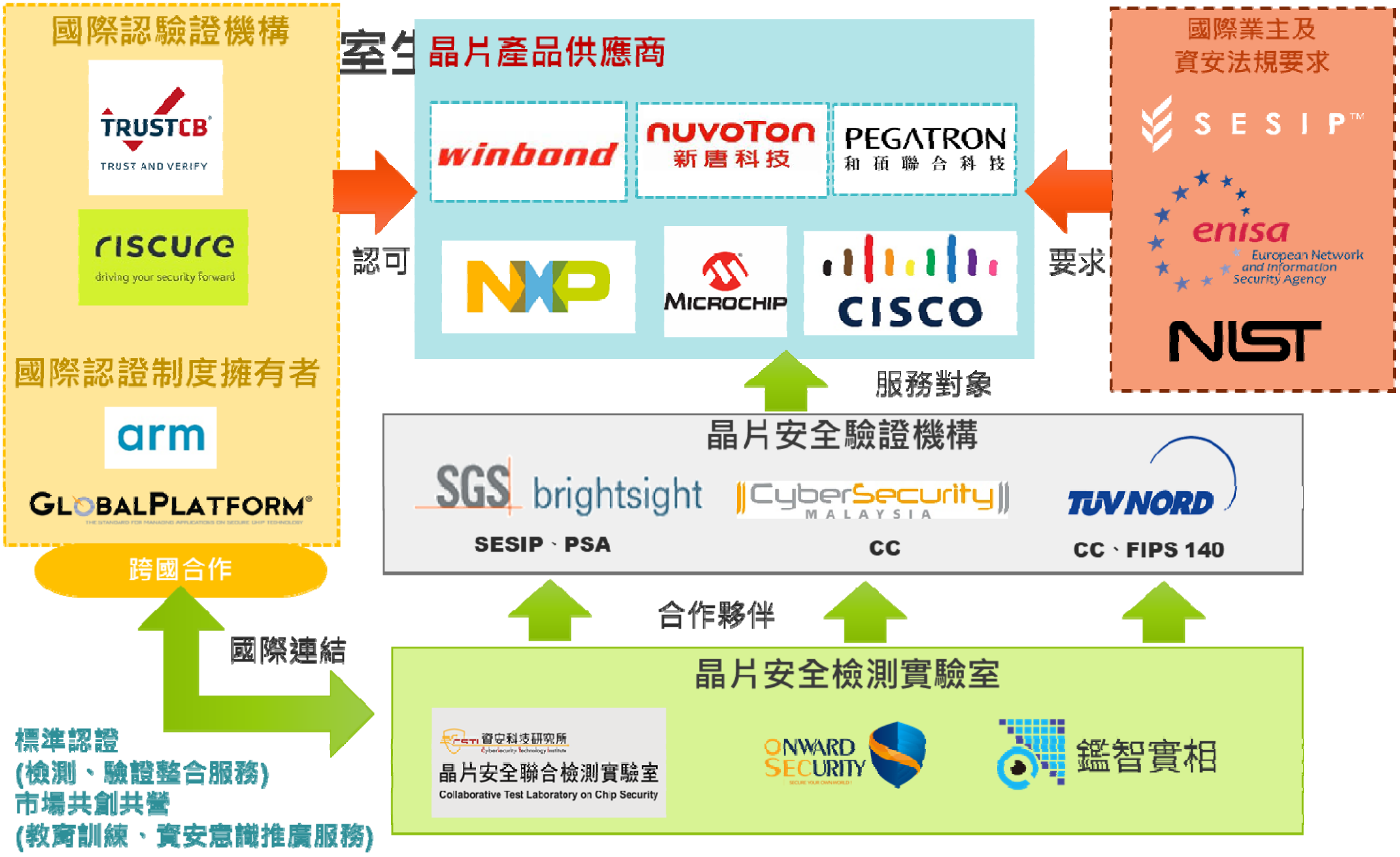
財團法人資訊工業策進會 INSTITUTE FOR INFORMATION INDUSTRY

SGS brightsight

國立中興大學 National Chung Hsing University

國立成功大學 National Cheng Kung University

推動安全檢測認驗證生態系



IC設計業者安全軟體開發成熟度

Why BSIMM

- 國內IC設計大廠自2019年起被國外買家進行安全開發成熟度稽核，諸多項目未能滿足買家之安全要求
- 有鑑於國內IC設計產業面臨國際合規要求之需要，資策會引進BSIMM 安全成熟度評估框架(Framework)，協助提升國內廠商之國際能見度及國際買家對於國內IC設計公司的品質信任度

SYNOPSYS®

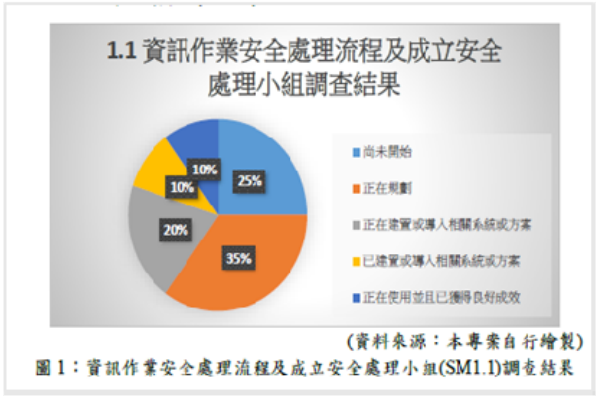
1. 自2008年，已對211家公司進行了約500次評估
2. V12包含來自128家公司數據
3. 為描述性模型，數據基於實時觀察結果
4. 描述業界正在做哪些事情，或已經做了哪些事情

推動成果

完成主要工作包括：推動IC設計業者安全成熟度自評、完成安全軟體發展參考指引修訂以協助業者與62443-4-1國際標準接軌，以及協助廠商示範導入並通過BSIMM國際評測。

安全軟體成熟度自評

累積推動30家IC設計業者進行安全軟體成熟度自評



(資料來源：本專案自行繪製)

圖 1：資訊作業安全處理流程及成立安全處理小組(SM1.1)調查結果

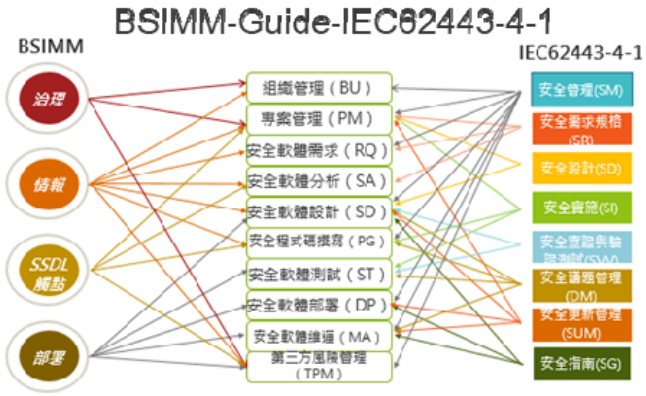
有55%業者已在收集及掌握新型態資安攻擊手法和漏洞等情報

約半數業者並未強制要求所有專案進行源碼審查

有六成業者尚未正式成立安全處理小組，未正式對內發佈作業安全處理流程

安全軟體開發參考指引

協助IC設計業者未來與IEC 62443-4-1國際驗證作準備



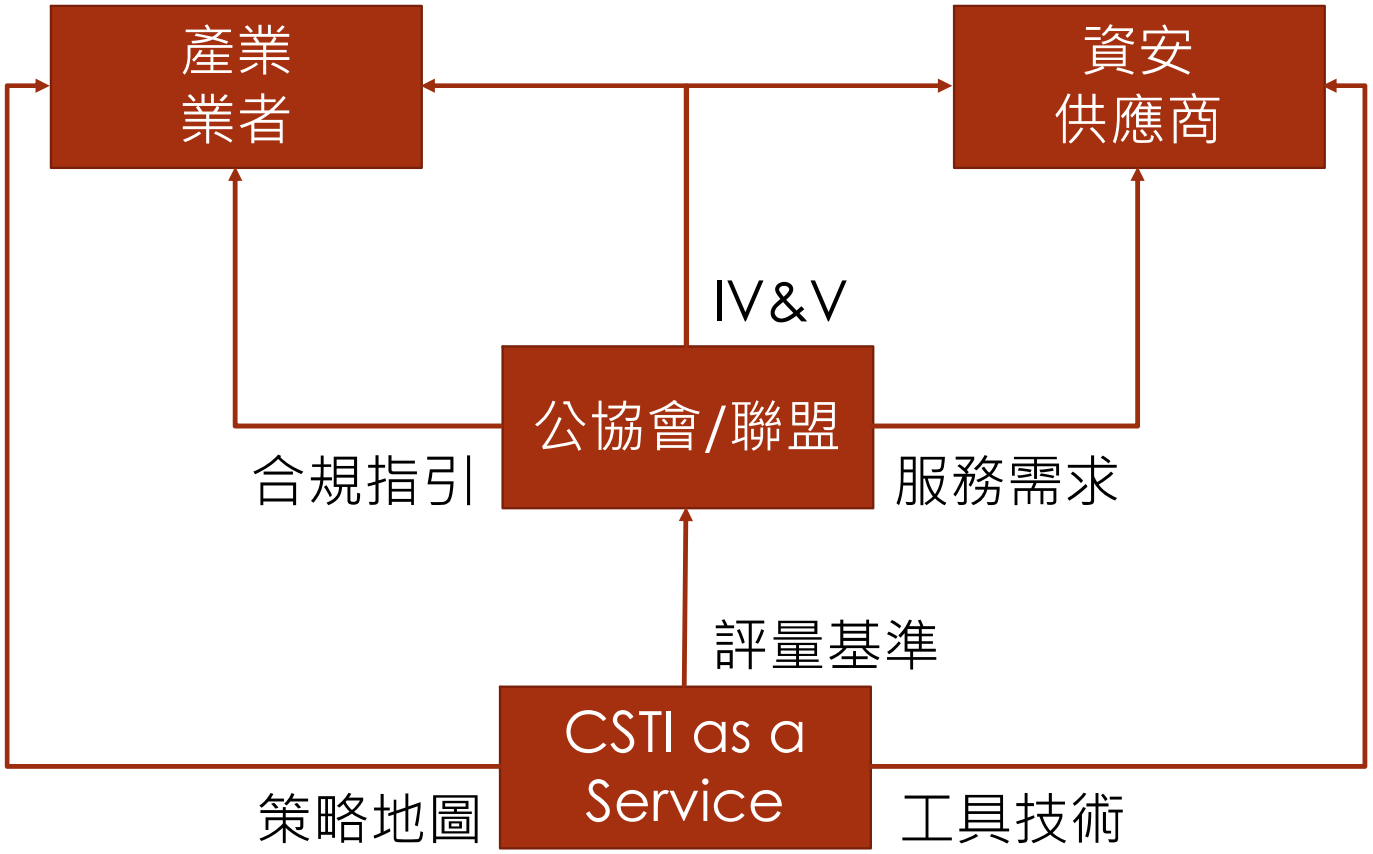
TEEMA邀集專家學者召開參考指引審查會議

輔導業者示範導入

輔導聯O、瑞O及神O通過BSIMM國際評測

未來合作建議

與公協會/聯盟合作共建聯防生態，提升業者因應資安之認知，增強與資安業者溝通能力



合作項目建議

晶片設計資安

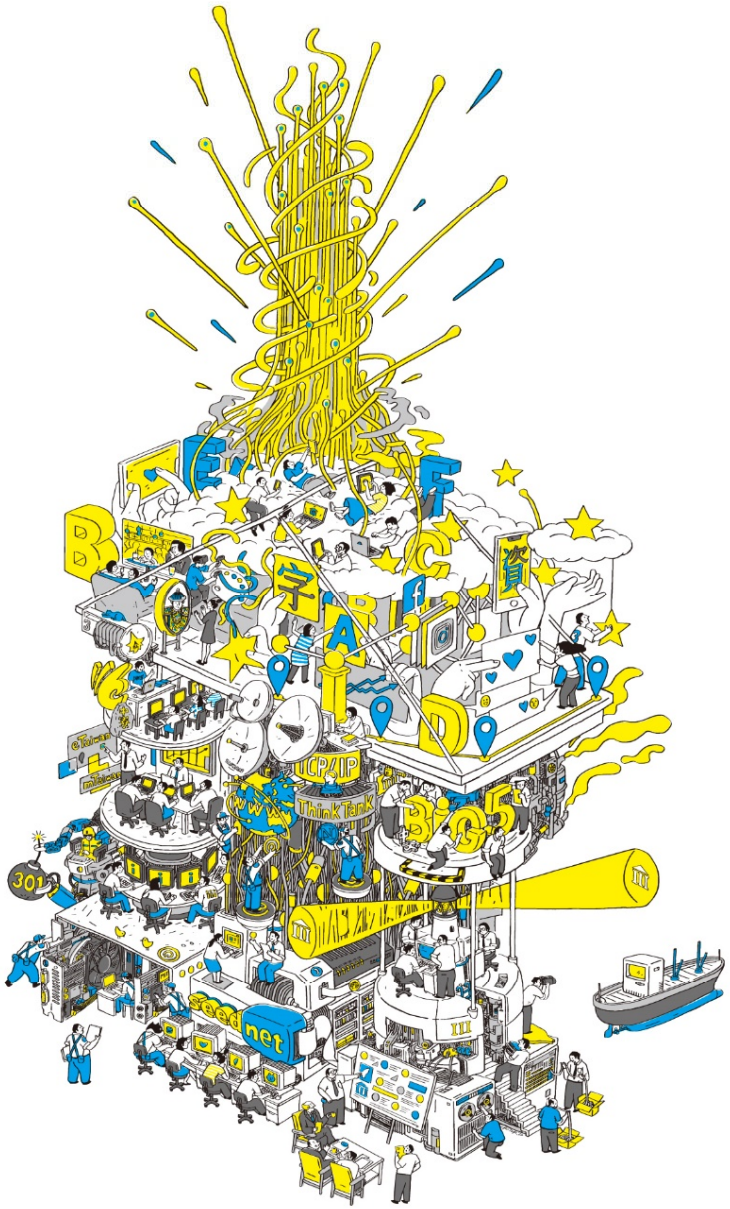
- 韌體檢測
- 硬體木馬檢測(實證)
- 晶片旁測道攻擊檢測(實證)
- 資安情資分享

產品資安合規

- 國際標準研究
- 檢測規範
- 產品安全檢測
- 國際認證

供應鏈安全

- 資安成熟度自評
- 導入BSIMM國際評核



1擘劃我國資訊工業發展藍圖 2開啟電腦中文化時代 3打造台灣資訊品牌 4培養台灣資訊人才
5開創產業顧問服務 6提升網路基礎建設 7E化政府系統 8普及網路應用人口
9建構資訊法案制度 10縮減城鄉數位落差 11推動數位內容 12推動數位科技外交
13策進 e-Taiwan / m-Taiwan 14精進5G智慧科技創新應用 15支援文創與設計產業奠基
16培育創新創業新動能 17擔任數位國家智庫 18活化原鄉無線寬頻環境
19協助產業拓展商機並強化資安防護 20數位轉型化育者

THANK YOU