台灣資通產業標準協會
Taiwan Association of Information and Communication Standards

物聯網資安測試實驗室一致性會議#9

TAICS 秘書處

2021.01.19

會議資訊

- **會議資訊：**
  - 會議時間：2021年 01月19日(二)下午 14:00~16:00
  - 會議地點： TAICS 第一會議室　台北市中正區北平東路30-2號6樓
- **會議主席：**台灣資通產業標準協會(TAICS)周勝鄰秘書長(陳曉強顧問代理)
- **出席代表：**
  - 經濟部工業局、財團法人工業技術研究院、財團法人資訊工業策進會
  - 認可實驗室：中華電信股份有限公司中華電信研究院、台灣德國萊因技術監護顧問股份有限公司、安華聯網科技股份有限公司、行動檢測服務股份有限公司、財團法人台灣商品檢測驗證中心、財團法人電信技術中心、勤業眾信聯合會計師事務所、資誠企業管理顧問股份有限公司、數聯資安股份有限公司
  - 廠商代表：Bosch (台灣博世) 、慧友電子股份有限公司

議程

一. 全盲(滲透性)測試導入網路攝影機資安驗證制度說明

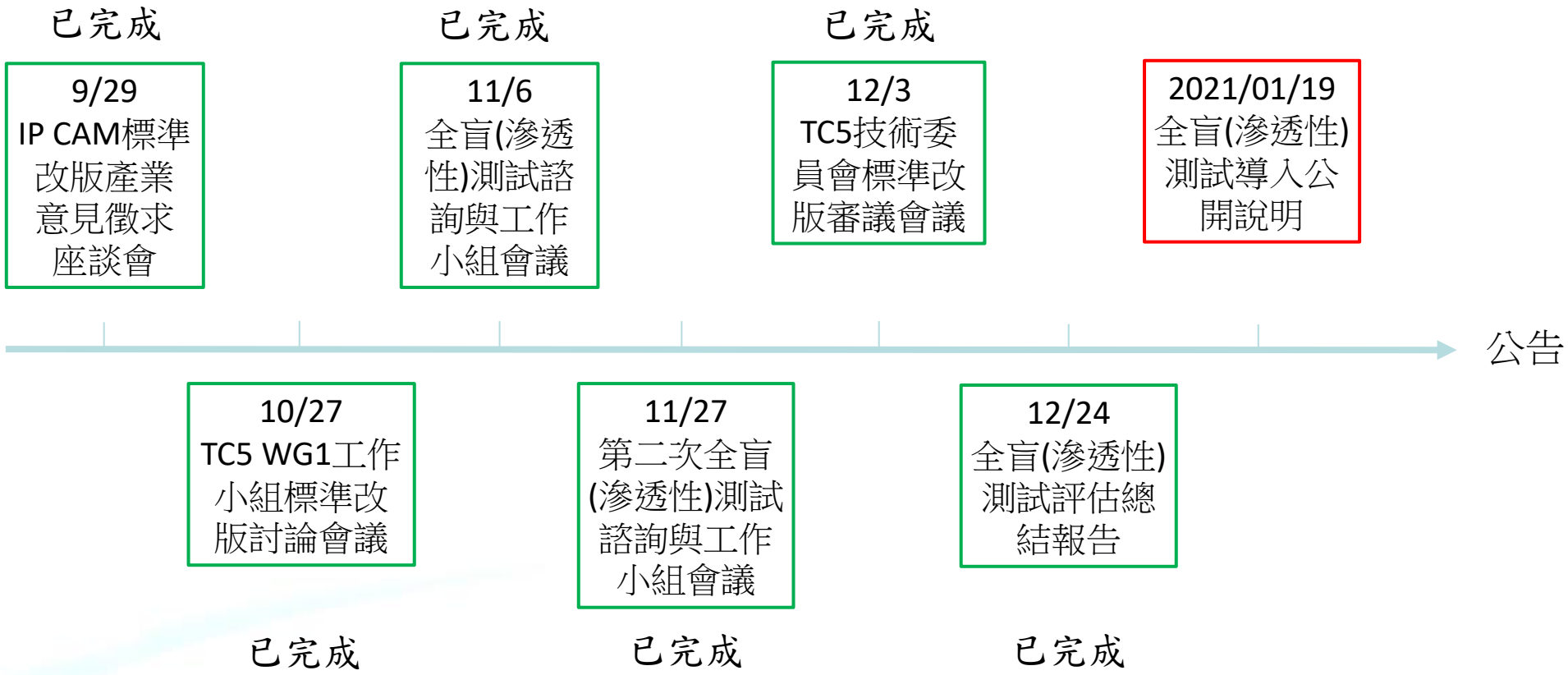
二. 系列認證

三. 能力試驗

四. 模糊測試

五. 臨時動議

IP CAM改版及全盲(滲透性)測試導入歷程



關鍵歷程

- **2020年09月29日 廠商意見徵詢座談會**
  - 會中決定，在可維持檢測結果一致性的情況下，於既有驗證制度導入全盲(滲透性)測試方法之應用。

- **2020年10月27日 TC5 WG1工作小組標準改版討論會議**
  - 實驗室或設備商可提出符合一致性做法的測項及測試方法，TAICS同時召集全盲(滲透性)測試諮詢與工作小組，依符合性評鑑原則逐條進行全盲(滲透性)測試可行性評估。

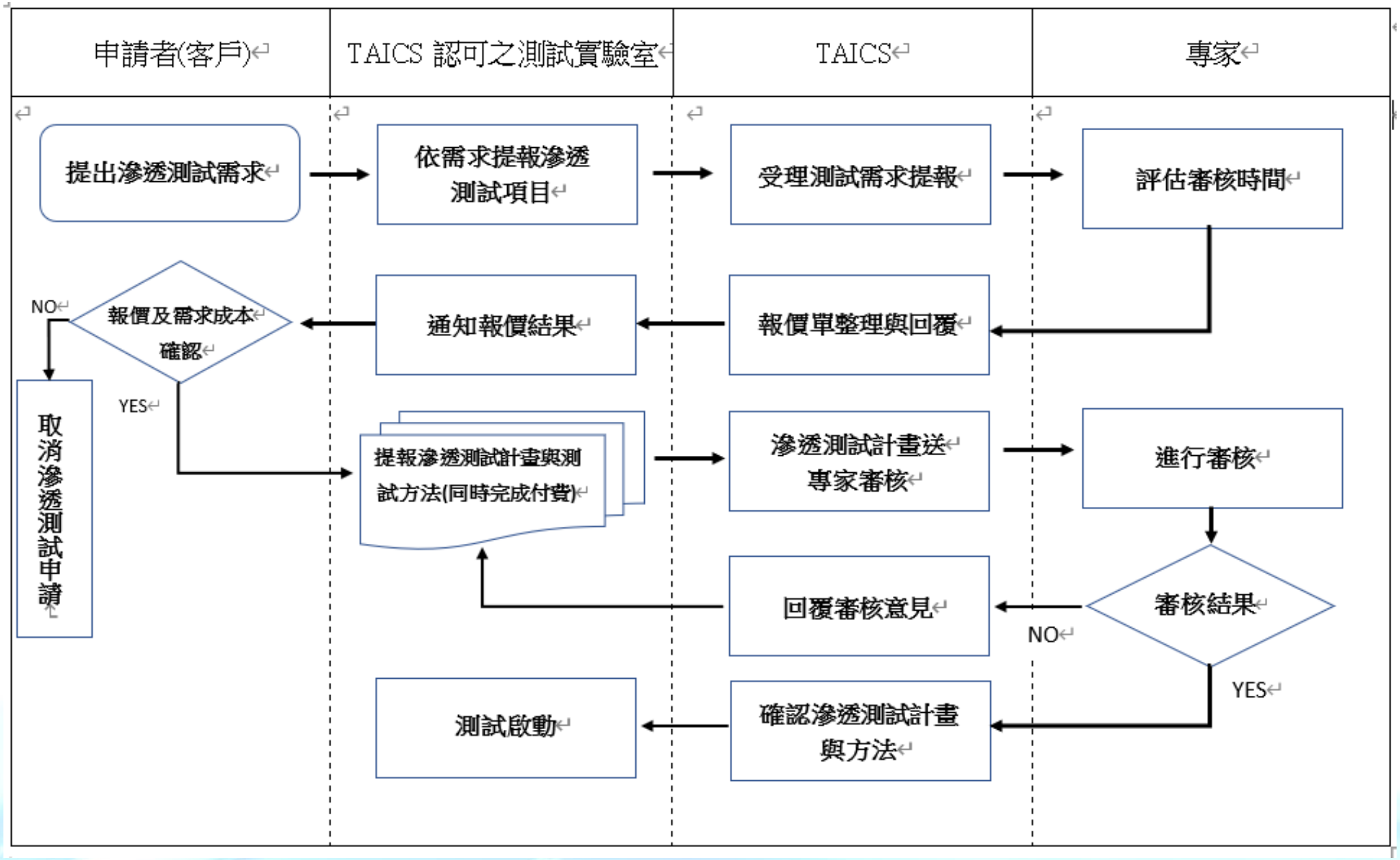
- **2020年11月6日 全盲(滲透性)測試諮詢與工作小組會議**
  - 經收集與整合全盲(滲透性)測試諮詢與工作小組成員個別最終評估結果，並依逾半數同意之適用條文於今日予以公開說明。

IP CAM改版及全盲(滲透性)測試導入效益

- 未來工業局主導之影像監控系統資安驗證制度，將可採用較多元之資安檢測方法。

- 實驗室應採用的檢測方法期能達成資安標準符合性評鑑之驗證需求，及檢測方法之確效。實驗室得依據TAICS TS-0015 series測試規範中的測試方法或本建議案進行資安檢測，以確保產品符合TAICS TS 0014-1及0014-2相關資安要求。

全盲(滲透性)測試導入建議流程



一、全盲(滲透性)測試導入網路攝影機資安驗證制度說明

驗證制度修正說明

- **變更部分**
  - 部分條文接受全盲(滲透性)測試方法之應用。
- **維持原檢測規範部分**
  - 原檢測規範即採用全盲(滲透性)測試或弱掃測試執行者。
- **不適用部分**
  - 經小組評估確認無法採用全盲(滲透性)測試方法者。

5.1.1.1實體介面安全管控測試

- **安全等級:**
  - 1級
- **評估結果:**
  - 可採用全盲滲透測試。
- **測試目的:**
  - 驗證是否可透過產品實體介面，存取作業系統之除錯模式。
- **測試方法:**
  - 當廠商宣告無法透過“實體介面”進入作業系統除錯模式時，則請廠商務必拉出debug pin來讓測試人員確認是否存在可存取OS的實體介面，實驗室可用邏輯分析儀、JTAG Emulator來驗證。

5.1.4.1 安全啟動(secure boot)測試

- **安全等級:**
  - 1、2、3級
- **評估結果:**
  - 可採用全盲滲透測試。
- **測試目的:**
  - 驗證產品於開機階段是否能確保產品之完整性及合法性。
- **測試方法:**
  - 1. 審閱具備安全啟動功能證明之書面資料，應至少包含(a)受信任私鑰列表是如何配置、(b)識別啟動過程會簽署到的程式，例: boot loader, 韌體, 及/或 軟體，及(c)安全啟動之運作方法
  - 2. 實驗室提供測試私鑰給受測廠商，請廠商使用該私鑰簽署受安全啟動保護的程式，例: boot loader, firmware, 及/或 software。
  - 3. 將產品重新啟動，檢視受測物是否能開機成功。
  - 4. 受測廠商將實驗室所提供之測試私鑰加入受測物之受信任私鑰列表。
  - 5. 將產品重新啟動，檢視受測物是否能開機成功

5.2.3.1(a) 韌體檔案安全測試

- **安全等級:**
  - 1、2、3級
- **評估結果:**
  - 可採用全盲滲透測試。
- **測試目的:**
  - 查驗產品具韌體更新功能。
- **測試方法:**
  - 請廠商提供韌體dump方法及介面，將韌體萃取出後執行逆向工程，若可還原出檔案系統格式，則查找敏感性資料是否存在；若無法還原出檔案系統格式，則採用16進位編輯器，檢視是否有可識別之敏感性資料。
  - 如果無法dump，廠商應提供加密韌體檔，先嘗試對加密的韌體進行解密，再進行本項測試驗證。

5.2.3.2 韌體更新檔之完整性及可信度測試

- **安全等級:**
  - 1、2、3級
- **評估結果:**
  - 可採用全盲滲透測試。
- **測試目的:**
  - 確認產品是否具備驗證韌體更新檔案完整性與不可否認性之能力。
- **測試方法:**
  - (1) 實驗室提供自簽公私鑰予送測廠商，廠商利用該私鑰簽署韌體，並將公鑰植入於產品。
  - (2) 實驗室執行韌體更新，檢視更新結果。
  - (3) 受測廠商將實驗室所提供之測試私鑰加入受測物之受信任私鑰列表。
  - (4) 實驗室執行韌體更新，檢視更新結果。

5.2.4.1、5.2.4.2 敏感性資料儲存安全測試

- **安全等級:**
  - 1、2、3級
- **測試目的:**
  - 驗證產品之敏感性資料於儲存狀態下是否加密保護。
- **評估結果:**
  - 不可採用全盲滲透測試。
- **理由:**
  - 廠商一旦加密或未開啟進入OS的介面，有很高的機率無法進行測試。

5.3.2.2 網路介面存取設置測試

- **安全等級:**
  - 1、2、3級
- **評估結果:**
  - 不可採用全盲滲透測試。
- **測試目的:**
  - 驗證產品是否可安全的透過遠端方式存取作業系統除錯模式之設計。
- **測試方法:**
  - 如果採用全盲測試，假使廠商有意隱藏，甚至必須使用特殊方法才能開啟遠端控制服務，則遠端連線方法是很難發現的(原方法還有廠商聲明佐證)。

其它一致性討論項目

二、系列驗證

- **系列產品之設定:**
  - 依申請者(及廠商)自行設定。

- **系列產品測試執行方法**
  - 系列產品一律加測網頁弱掃、系統弱掃(避免configuration改動造成的影響)。
  - 外觀或電路板上配置不同，實體安全亦須加測

- **系列產品驗證所需測試項目，除上項規定外，皆委由認可實驗室依系列產品與原登錄主產品差異點可能衍生資安風險與標準條文確認與執行。**

  TAICS將於審驗階段依其必要性建議加測驗證項目。然為能提供申請者較簡便之服務及建立與認可實驗室互信與相互學習之連結，除具迫切且重點差異點須驗證與加測外，皆以觀察(Observation)事項予以建議或輕微(Minor)事項要求文書回覆即可。此類案例將納入定期一致性會議與認可實驗室分享。

三、能力比對試驗

- **舉辦時間**
  - 預計2021 Q3

- **舉辦方法**
  - 對象: 所有IP CAM認可實驗室。
  - 依比對採購數量採Round-robin模式或同時寄件至所有實驗室執行之。
  - 參與實驗室能力比對測試須繳交測試費用，費用金額將與報名簡章同時公告之。

- **結果**
  - 協會將委請中心實驗室進行測試與比對分析，並以實驗室匿名方式發行能力比對試驗報告以利參與實驗室自行研讀與檢討。
  - 實驗室須提出矯正預防措施。
  - 未參加年度能力比對測試之認可實驗室將不受理認可實驗室延展申請。

四、模糊測試

- **根據2020.01.09，TAICS #6驗證一致性會議決議，模糊測試工具維護成本高，在資安測試市場未達到一定規模時，難以支撐。**

- **當日會後決議**
  - 接受委外測試，且委託實驗室須具TAF或ILAC認證實驗室執行之。

- **實際做法**
  - 未來2、3級實驗室若不具備fuzzing的測試能力，將會註明在 TAF證書上。
  - 測試報告必須註明fuzzing相關測項不在TAF認可範圍。

臨時動議