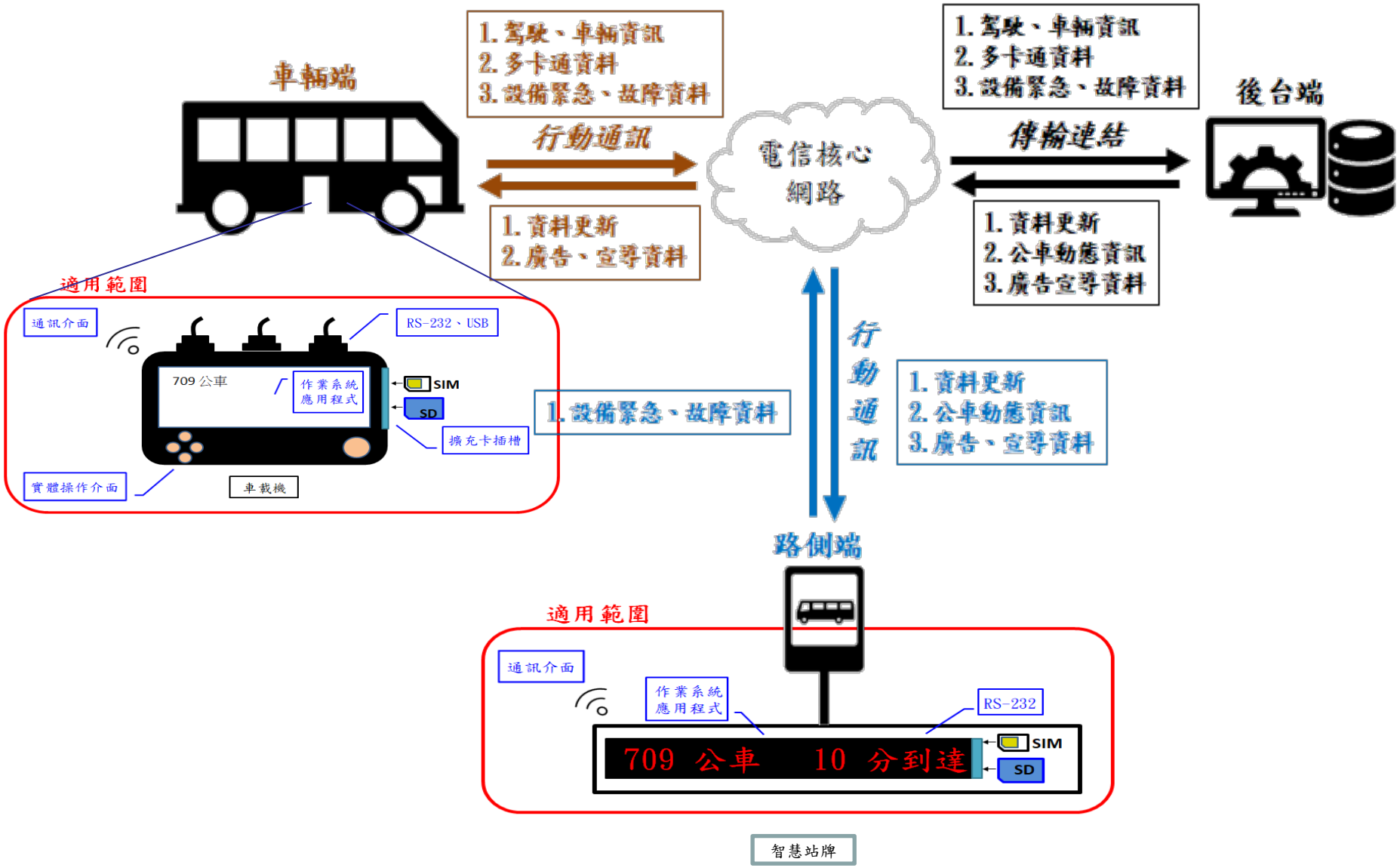
智慧巴士資通訊系統系列
資安標準簡介

李岳翰

資策會 資安所 聯網安全檢測組

標準適用範圍


車輛端
1. 駕駛、車輛資訊
2. 多卡通資料
3. 設備緊急、故障資料
行動通訊
1. 資料更新
2. 廣告、宣導資料
電信核心網路
1. 駕駛、車輛資訊
2. 多卡通資料
3. 設備緊急、故障資料
傳輸連結
1. 資料更新
2. 公車動態資訊
3. 廣告宣導資料
後台端
適用範圍
通訊介面
RS-232、USB
709 公車
作業系統應用程式
SIM
SD
擴充卡插槽
實體操作介面
車載機
1. 設備緊急、故障資料
行動通訊
1. 資料更新
2. 公車動態資訊
3. 廣告、宣導資料
路側端
適用範圍
通訊介面
作業系統應用程式
RS-232
709 公車 10 分到達
SIM
SD
智慧站牌

安全分級

- 1級: 適用RTOS、Non-OS這種功能簡易之車載機、智慧站牌。
- 2級: 適用well-known OS，例如: windows、Linux、Android等，這種裝載眾所周知作業系統之車載機、智慧站牌。
- 3級: 適用well-known OS，且應用於自駕環境所需的車載機、智慧站牌，所必須達到的基本安全要求

一般要求

5.1.1.1
作業系統安全與網路服務安全測試(2級)

- **測試目的：**
  - 測試作業系統是否存在CVSS v3 評分為7.0分以上之常見資安弱點與漏洞。
- **測試時間：**
  - 中(30分鐘以內)。
- **注意：**
  - 漏洞嚴重性評比是以NVD網站為主，而不是工具。
  - 要求廠商給予最高權限帳號，進行登入檢測。
- **正確結果：**
  - 作業系統層最高權限帳號，漏洞的CVSS v3為7分以下
- **測試複雜度：**
  - 易(工具)

5.1.1.2
測試未經授權軟體是否可以安裝及執行(2級)

- **測試目的：**
  - 驗證產品是否限制未經授權軟體的安裝及執行。
- **測試時間：**
  - 中(30分鐘以內)。
- **注意：**
  - 可自行安裝軟體功能關閉。
  - 或者鎖定在特定應用程式上。
  - 連透過debug port都不行安裝。
- **正確結果：**
  - 未經授權的軟體無法被安裝及執行
- **測試複雜度：**
  - 易

5.1.2.1
網路服務最小化測試(1級)

- **測試目的：**
  - 驗證產品是否存在預期以外之網路埠。
- **測試時間：**
  - 冗長(超過8小時)。
- **注意：**
  - 必須要驗證動態埠、TCP、UDP。
  - 廠商必須自我宣告所開啟的網路埠。
- **正確結果：**
  - 實驗室所檢測到開啟的網路埠必須與廠商宣告一致。
- **測試複雜度：**
  - 易(工具)

5.1.3.1
韌體更新測試(1級)

- **測試目的：**
  - 驗證產品韌體是否具備更新機制。
- **測試時間：**
  - 短(10分鐘內)。
- **注意：**
  - 此測項指的韌體是僅限於RTOS及Non-OS的韌體
  - Well-known OS的韌體不在此限制中
- **正確結果：**
  - 產品具備韌體更新機制。
- **測試複雜度：**
  - 易

5.1.3.2
應用程式更新測試(2級)

- **測試目的：**
  - 驗證產品應用程式是否具備更新機制，以及更新失敗時，是否回復至更新版本前之狀態。
- **測試時間：**
  - 短(10分鐘內)。
- **注意：**
  - 跟5.1.3.1測項類似，差異僅在對象為執行TTIA產業標準所定義功能之應用程式
- **正確結果：**
  - 產品具備應用程式更新機制。
  - 若更新失敗，產品仍可回復至更新版本前之狀態。
- **測試複雜度：**
  - 易

5.1.3.3
作業系統更新測試(3級)

- **測試目的：**
  - 驗證產品作業系統是否具備更新機制，以及更新失敗時，是否回復至更新版本前之狀態。
- **測試時間：**
  - 短(10分鐘內)。
- **注意：**
  - 此測項的對象僅限於Well-known OS
- **正確結果：**
  - 產品具備作業系統更新機制。
  - 若更新失敗，產品仍可回復至更新版本前之狀態。
- **測試複雜度：**
  - 易

5.1.3.4
更新檔之完整性測試(1級)

- **測試目的：**
  - 驗證產品軟韌體更新是否驗證更新檔的完整性。完整性驗證功能須採用FIPS PUB 140-2 Annex A[1]所核可之雜湊(hash)演算法。
- **測試時間：**
  - 短(10分鐘內)。
- **注意：**
  - 必須採用FIPS PUB 140-2 Annex A所核可之雜湊(hash)演算法。
  - 無論手動或線上更新擇一測試即可，手動更新對實驗室會更好做。
- **正確結果：**
  - 產品更新失敗。
- **測試複雜度：**
  - 中

5.1.3.5
更新檔之合法性測試(3級)

- **測試目的：**
  - 驗證產品軟體更新是否驗證更新檔的合法性。合法性驗證功能須採用FIPS PUB 140-2 Annex A[1]所核可之簽章演算法。
- **測試時間：**
  - 短(10分鐘內)。
- **注意：**
  - 必須採用FIPS PUB 140-2 Annex A所核可之簽章演算法。
  - 無論手動或線上更新擇一測試即可，手動更新對實驗室會更好做。
- **正確結果：**
  - 產品更新失敗。
- **測試複雜度：**
  - 中

5.1.4.1
安全事件紀錄測試(1級)

- **測試目的：**
  - 驗證事件紀錄是否具時間戳記及事件內容。
- **測試時間：**
  - 短(10分鐘內)。
- **注意：**
  - 這裡指的是「安全事件」日誌，而不是一般的系統日誌。
  - 安全事件日誌不得因為重新開機而被清除。
  - 該日誌存放於後台者要附上佐證資料供審查。
- **正確結果：**
  - 產品提供安全事件日誌，且日誌內包含時間戳記及事件內容。
- **測試複雜度：**
  - 易

5.1.4.2
安全事件紀錄日誌檔之日誌滾動功能測試(1級)

- **測試目的：**
  - 驗證產品是否具備處理日誌儲存空間不足之異常狀況。
- **測試時間：**
  - 冗長(8小時以上，視日誌存放容量)。
- **注意：**
  - 測試對象是安全事件日誌，其它行為(例:錄影)造成儲存空間不足，不在本測項中。
  - 實驗室應該要有自動化的測試工具，以增加測試可執行之可信度。
- **正確結果：**
  - 產品不會發生儲存空間不足的現象。
  - 產品仍可正常記錄安全事件。
- **測試複雜度：**
  - 易。

5.1.4.3
產品異常警示功能測試(1級)

- **測試目的：**
  - 驗證產品發生異常時，是否進行推播或告警等警示機制。
- **測試時間：**
  - 短(10分鐘以內)。
- **注意：**
  - 觸發產品定義之異常事件，如中斷網路，或網路遮罩。
- **正確結果：**
  - 產品發生異常狀態時，發出推播或告警等警示機制。
- **測試複雜度：**
  - 易。

5.1.5.1
敏感性資料權限管控測試(2級)

- **測試目的：**
  - 驗證產品所儲存的安全敏感性資料，是否經授權方可存取。
- **測試時間：**
  - 中(30分鐘以內)。
- **注意：**
  - 受測廠商須提供一版可進入作業系統層最高權限帳號之產品。
- **正確結果：**
  - (1) 存取權限有區分為使用者、管理者。
  - (2) 產品所儲存的安全敏感性資料，須經管理者權限授權方可存取。
- **測試複雜度：**
  - 中等

5.1.5.2
敏感性資料加密儲存測試(2級)

- **測試目的：**
  - 驗證產品是否加密儲存安全敏感性資料，且加密方式是否採用FIPS PUB 140-2 Annex A所核可之演算法。
- **測試時間：**
  - 長(30分鐘以上)。
- **注意：**
  - 受測廠商須提供一版可進入作業系統層高權限帳號之產品。
- **正確結果：**
  - 安全敏感性資料的保密機制採用FIPS 140-2 Annex A所核可之加密演算法。
- **測試複雜度：**
  - 中等

5.1.6.1
網頁管理介面常見資安風險測試(2級)

- **測試目的：**
  - 驗證產品之網頁管理介面是否存在已知資安漏洞。
- **測試時間：**
  - 長(30分鐘以上，不同產品會有不同的反應時間)。
- **注意：**
  - 絕大部份使用工具。
  - 必須是登入網頁管理介面的狀態下(且為系統管理者權限)，執行測試。
- **正確結果：**
  - 網頁管理介面，不存在引發OWASP web Top 10之Injection及XSS資安攻擊風險。
- **測試複雜度：**
  - 易(工具)

5.2.1.1
資料完整性與驗證其來源測試(3級)

- **測試目的：**
  - 驗證資料傳輸是否透過數位簽章來確保資料的完整性與驗證其來源。
- **測試時間：**
  - 中(30分鐘以內)。
- **注意：**
  - 需搭配後台伺服器才能測試，必須請送測廠商觸發附錄B，TTIA所參照的運研所97年度公車動態資訊。
  - 測試對象是前端設備
- **正確結果：**
  - 傳輸遭竄改過的資料，不被前端設備(車載機、智慧站牌)所接收。
- **測試複雜度：**
  - 中等

5.2.2.1
安全敏感性資料之傳輸保護測試(1、3級)

- **測試目的：**
  - 驗證產品傳輸安全敏感性資料是否加密，且加密方式是否採用FIPS PUB 140-2 Annex A所核可之加密演算法。
- **測試時間：**
  - 中(30分鐘以內)。
- **注意：**
  - 有2個級數的測試，1級測的是RF通訊該段，即前端設備到接入端裝置；3級測的是後端鏈路，即ethernet那段。
  - RF段，測的是4G傳輸有沒有加密，如果是透過Wi-Fi，則5.2.4章節會測到。Ethernet段，測的是傳輸走TLS安全通道。
- **正確結果：**
  - 初階(1級): RF段傳輸加密。
  - 中階(3級): Ethernet段傳輸走安全通道。
- **測試複雜度：**
  - 高

5.2.3.1
產品資料傳輸測試(1級)

- **測試目的：**
  - 驗證產品資料傳輸時，是否將資料傳輸到非認可之傳輸對象。
- **測試時間：**
  - 長(30分鐘以上)。
- **注意：**
  - 廠商必須宣告合法的伺服器。
  - 附錄B，TTIA所參照的運研所97年度公車動態資訊。
- **正確結果：**
  - 傳輸對象與產品宣告一致。
- **測試複雜度：**
  - 難

5.2.4.1
安全的Wi-Fi 組態設置測試(1級)

- **測試目的：**
  - 驗證產品是否存在錯誤的Wi-Fi設定。
- **測試時間：**
  - 短(10分鐘以內)。
- **注意：**
  - 無。
- **正確結果：**
  - 有提供使用者 WPS PIN 開/關之功能。
  - WPS PIN 功能預設為關閉。
- **測試複雜度：**
  - 易

5.2.4.2
Wi-Fi網路之Wi-Fi保護設置測試(1級)

- **測試目的：**
  - 驗證產品Wi-Fi網路之Wi-Fi保護設置是否使用v2同等或以上之版本。
- **測試時間：**
  - 中(30分鐘以內)。
- **注意：**
  - 無。
- **正確結果：**
  - 產品之Wi-Fi保護設置使用v2同等或以上之版本。
- **測試複雜度：**
  - 易

5.2.4.3
Wi-Fi通訊協定異常輸入測試(2級)

- **測試目的：**
  - 驗證產品之 Wi-Fi 通訊協定是否存在未知之資安漏洞。
- **測試時間：**
  - 冗長(8小時以上，不同產品會有不同的反應時間)。
- **注意：**
  - 工具檢查監控產品是否仍正常運作。
- **正確結果：**
  - 產品於測試過程中不會因為某一特定異常封包而發生程序崩潰(crash)。
- **測試複雜度：**
  - 易(工具)

車載機

5.3.1.1
產品擴充卡插槽防護示警測試(1級)

- **測試目的：**
  - 驗證產品擴充卡插槽是否具保護措施，以及保護遭移除時是否具可辨識性或示警功能。
- **測試時間：**
  - 極短。
- **注意：**
  - 至少要達到可辨識擴充卡曾被移除的效果。
- **正確結果：**
  - 擴充卡插槽具保護措施。
  - 保護措施遭拆解時，產品外觀可輕易辨識，或通知管理者、推播警示或告警訊息。
- **測試複雜度：**
  - 易

5.3.1.2
產品外殼拆解測試(1級)

- **測試目的：**
  - 驗證產品外殼防拆機制若遭拆解是否具可被辨識之功能。
- **測試時間：**
  - 極短。
- **注意：**
  - 至少要達到可辨識外殼曾被移除的效果。
- **正確結果：**
  - 產品外殼經拆解後，防拆機制應可被辨識已被拆解且無法復原。
- **測試複雜度：**
  - 易

5.3.2.1
產品實體連接介面安全管控測試(1級)

- **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。
- **測試時間：**
  - 中(30分鐘內)。
- **注意：**
  - 有可能燒壞待測設備或測試工具的風險。
  - 實驗室應提前準備好介接工具。
  - 受測單位須告知Debug埠的位置，受測單位希望不要隱瞞，實驗室必須要有能力找尋Debug埠的能力。
- **正確結果：**
  - 不存在debug port。
  - Debug port接上去，console沒反應。
  - Debug port接上去，console顯示要求認證，且符合5.4.2節的所有要求。
- **測試複雜度：**
  - 中等

5.4.1.1
產品實體操作介面測試(1級)

- **測試目的：**
  - 驗證產品透過實體操作進入除錯模式是否具身分鑑別之功能。
- **測試時間：**
  - 短(10分鐘內)。
- **注意：**
  - 是指可以從實體按鍵進入debug mode的情況。
- **正確結果：**
  - 經過身分鑑別機制，方可進入除錯模式；或者產品不提供透過實體按鍵進入除錯模式之功能。
  - 採用的通行碼鑑別機制，符合5.4.2.1的要求。
- **測試複雜度：**
  - 中等

5.4.1.2
身分鑑別錯誤訊息測試(1級)

- **測試目的：**
  - 驗證鑑別錯誤訊息不會造成敏感性資料的洩漏。
- **測試時間：**
  - 短(10分鐘內)。
- **注意：**
  - 當認證資料輸入錯誤時，只要回覆「身分鑑別失敗」或「帳號或密碼輸入錯誤」即可。
  - 網頁介面、RESTful API
- **正確結果：**
  - 從鑑別錯誤訊息無法推斷出合法使用者名稱。
- **測試複雜度：**
  - 易

5.4.1.3
鑑別機制強度測試(2級)

- **測試目的：**
  - 驗證產品是否具備可靠之身分鑑別機制。
- **測試時間：**
  - 中(30分鐘以內)。
- **注意：**
  - 網頁管理介面。
- **正確結果：**
  - 身分鑑別機制具備抵抗重送攻擊的能力。
  - 登出後確實須再次登入，方可存取產品。
- **測試複雜度：**
  - 易

5.4.1.4
身分鑑別輸入頻率及次數限制測試(2級)

- **測試目的：**
  - 驗證身分鑑別機制是否有防止暴力破解之能力。
- **測試時間：**
  - 短(10分鐘內)。
- **注意：**
  - 無。
  - 網頁管理介面。
- **正確結果：**
  - 輸入次數5次以內，會鎖定帳戶。
  - 於廠商宣告之帳戶鎖定時限內，帳戶未解除鎖定。
  - 於廠商宣告計數器重設時限內，失敗次數未重新計算。
- **測試複雜度：**
  - 易

5.4.2.1 通行碼長度測試(1級)

- **測試目的：**
  - 驗證產品的通行碼長度是否足夠，以確保其強度。
- **測試時間：**
  - 短(10分鐘內)。
- **注意：**
  - 無。
  - 網頁管理介面。
- **正確結果：**
  - 無法建立或變更小於8 個字元長度之通行碼。
- **測試複雜度：**
  - 易

5.4.2.2 通行碼複雜度測試(2級)

- **測試目的：**
  - 驗證產品的通行碼複雜度是否足夠，以確保其強度。
- **測試時間：**
  - 短(10分鐘內)。
- **注意：**
  - 選其中3種實作就行。
  - 網頁管理介面。
- **正確結果：**
  - 通行碼中之字元必須符合下列四種字元中的三種，1.英文大寫字元 (A 到 Z)；2.英文小寫字元 (a 到 z)；3.10 進位數字 (0 到 9)；4.非英文字母字元 (例如：！、$、#、%)。
- **測試複雜度：**
  - 易

5.4.3 權限管控機制(1級)

- **測試目的：**
  - 驗證產品資源的存取是否具有權限控管機制。
  - 驗證產品是否存在有限的授權時間長度。
- **測試時間：**
  - 中等或更短。
- **注意：**
  - 透過網頁管理介面或實體連接介面。
- **正確結果：**
  - 該權限管控機制至少擁有二個以上不同權限的角色。
  - 產品之授權行為，存在閒置時限供使用者設定。
  - 遠端連線閒置逾時，須經過身分鑑別方可存取產品。
- **測試複雜度：**
  - 易

智慧站牌

5.1.1.2
產品啟動測試(1級)

- **測試目的：**
  - 驗證系統開機啟動時不會洩漏任何硬體相關的唯一識別資訊。
- **測試時間：**
  - 短(10分鐘內)。
- **注意：**
  - 唯一識別資訊即IMSI、IMEI。
- **正確結果：**
  - 畫面未顯示任何唯一識別資訊。
- **測試複雜度：**
  - 易

5.3.1.1
實體保護測試(1級)

- **測試目的：**
  - 驗證產品是否建立外殼拆除障礙。
- **測試時間：**
  - 極短(1分鐘內)。
- **注意：**
  - 無。
- **正確結果：**
  - 不可使用一般十字或一字螺絲。
- **測試複雜度：**
  - 易

5.3.1.2
實體防護告警測試(3級)

- **測試目的：**
  - 驗證產品是否建立外殼拆除障礙。
- **測試時間：**
  - 短(10分鐘內)。
- **注意：**
  - 無。
- **正確結果：**
  - 產品外殼遭拆卸時，產品有具備相關警示機制。
- **測試複雜度：**
  - 易

Thank You