TAICS

TAICS TS-0021-2 v2.0 : 2019

智慧巴士資通訊系統資安測試規範－第二部：車載機v2

Intelligent Bus Telematics System Security Test Specification - Part 2: On Board Unit v2

2019/08/13

社團法人台灣資通產業標準協會

Taiwan Association of Informationand Communication Standards

智慧巴士資通訊系統資安測試規範

-第二部：車載機 v2

Intelligent Bus Telematics System Security Test Specification

- Part 2: On Board Unit v2

出版日期: 2019/08/13

終審日期: 2019/07/26

誌謝

本規範由台灣資通產業標準協會－TC5 網路與資訊安全技術工作委員會所制定。

TC5 主席：安華聯網科技股份有限公司 洪光鈞 總經理

TC5 主席：神盾股份有限公司 張心玲 副總經理

TC5 副主席：財團法人資訊工業策進會 蔡正煜 副主任

TC5 物聯網資安工作組組長：財團法人資訊工業策進會 高傳凱 博士

TC5 物聯網資安工作組：財團法人資訊工業策進會 李岳翰

財團法人資訊工業策進會 林志濰

此標準制定之協會會員參與名單為(以中文名稱順序排列)：

中華電信股份有限公司、互聯安睿資通股份有限公司、台灣車聯網產業協會、安華聯網科技股份有限公司、行動檢測服務股份有限公司、果核數位股份有限公司、財團法人工業技術研究院、財團法人台灣電子檢驗中心、財團法人資訊工業策進會、財團法人電信技術中心、國立交通大學、趨勢科技股份有限公司。

本計畫專案參與廠商(法人)名單為(以中文名稱順序排列)：

中華資安國際股份有限公司、用新科際整合有限公司、亞旭電腦股份有限公司、松穎科技股份有限公司、研華股份有限公司、國立雲林科技大學、晶復科技股份有限公司、極星國際航電股份有限公司、銓鼎科技股份有限公司、慧友電子股份有限公司、馥鴻科技股份有限公司、寶錄電子股份有限公司、寶儷明股份有限公司。

本規範由經濟部工業局支持研究制定。

目錄

前言

本規範係依台灣資通產業標準協會(TAICS)之規定，經技術管理委員會審定，由協會公布之產業規範。

本規範並未建議所有安全事項，使用本規範前應適當建立相關維護安全與健康作業，並且遵守相關法規之規定。

本規範之部分內容，可能涉及專利權、商標權與著作權，協會不負責任何或所有此類專利權、商標權與著作權之鑑別。

引言

隨著硬體設備以及網路傳輸快速進步，物聯網應用已進入蓬勃發展階段。經濟部工業局於 2017 年宣示進入物聯網資安產業標準元年，致力於推動資安以及其檢測標準，包括影像監控系統資安標準、車聯網系統資安標準、物聯網通用資安標準、輔助應用程式資安標準、工控系統資安標準、醫療儀器資安標準及銷售點終端系統資安標準等，藉由資安標準訂定，國內物聯網產業能將產品優質化並更具有競爭力。智慧巴士為車聯網的子項目，且目前公車產業已有八成公車(約兩萬兩千輛)已轉換為智慧巴士，而公車做為交通基礎建設一部份，每年各縣市政府也會持續維護並更新公車相關軟硬體設備。因此為防範日益增多的車聯網資安事件，例如巴西 Curitiba City 巴士總站與中國麗水市內的智慧站牌遭不明入侵播放色情影片，以及美國舊金山交通運輸系統遭駭停擺，導致市政府不得不免費讓民眾搭乘直到系統修復為止等，希望藉由「智慧巴士資通訊系統資安測試規範－第二部：車載機」之制定(以下簡稱本測試規範)，建立國內智慧巴士車載機之資安品質標準測試規範，使產品商或系統服務商在產品研發上有所依據，藉以促進國內產業整體優質化及產品競爭力，並確保其使用的資訊安全。

本測試規範乃配合「台灣資通產業標準協會」(Taiwan Association of Information and Communication Standards，以下簡稱 TAICS)制定之 TAICS TS-0020-2「智慧巴士資通訊系統資安標準－第二部：車載機」標準所訂定，其中具體明列資安檢測之測試項目、測試條件、測試方法及預期結果等事項；並確保測試程序的完整性及測試資料的一致性。結合另一份測試規範，TAICS TS-0021-1「智慧巴士資通訊系統資安測試規範－第一部：一般要求」，就可成為相關產品開發與資安檢測的參考藍本。

本規範因應 TS-0020-2 版本更新，進行文件內容改版。改版內容將安全要求加入分級制度、增加網路管理介面及權限管控安全要求，另對原測試規範內容進行調整。改版差異請見版本修改紀錄。

1. 適用範圍

本測試規範依據 TAICS TS-0020-2「智慧巴士資通訊系統資安標準－第二部：車載機」訂定，適用於下述產品之資安檢測：安裝於座位在十人座以上或總重量逾三千五百公斤之營業用大客車、座位在二十五人座以上或總重量逾三千五百公斤之幼童專用車上，主要功能以行車資訊串接、安全輔助、駕駛輔助及車輛管理輔助為目的之車載機產品。

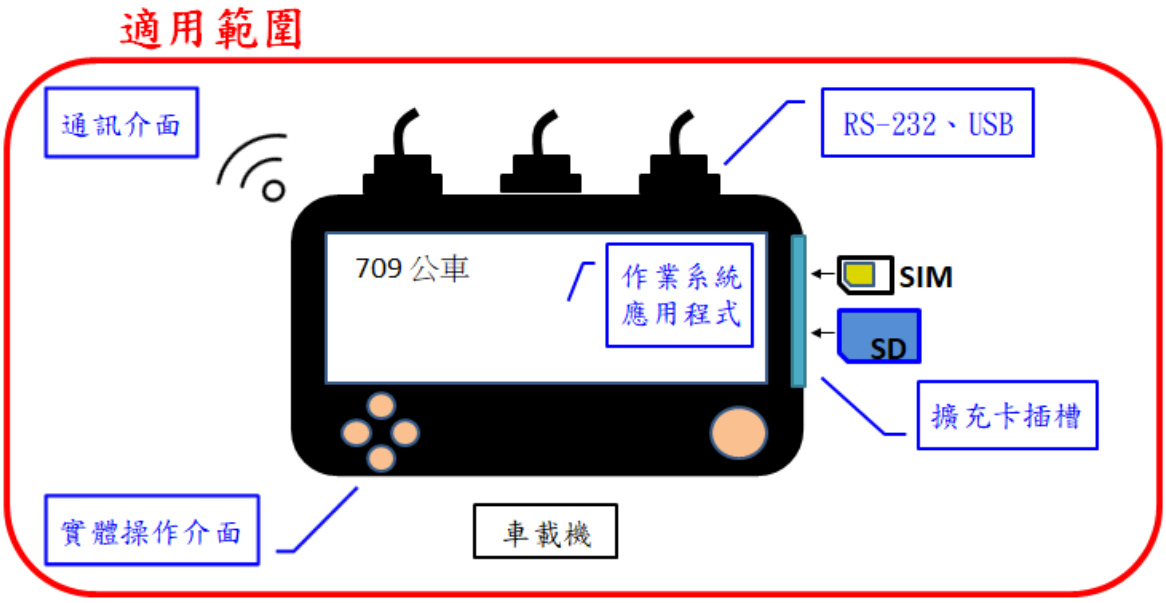

圖 1 適用範圍示意圖

2. 引用標準

以下引用標準係本標準必要參考文件。如所列標準標示年版者，則僅該年版標準予以引用。未標示年版者，則依其最新版本(含補充增修)適用之。

TAICS TS-0020-2 「智慧巴士資通訊系統資安標準－第二部：車載機」

TAICS TS-0021-1 「智慧巴士資通訊系統資安測試規範－第一部：一般要求」

台灣車聯網產業協會 「營業大客車車載機產業標準」V2.0

3. 用語及定義

TAICS TS-0020-2「智慧巴士資通訊系統資安標準－第二部：車載機」所規定之用語及定義適用於本規範。

4. 測試項目

本節依據 TAICS TS-0020-2 v2.0「智慧巴士資通訊系統資安標準－第二部：車載機」制定相對應之安全測試項目及測試方法。

實機測試總表，如表 1 所示，第一欄為安全構面，包括：(1)系統安全、(2)通訊安全、(3)實體安全、(4)身分鑑別與授權機制安全；第二欄為安全要求分項，係依第一欄安全構面設計對應之安全測試項目；第三欄為安全等級。本實機測試總表，須依循章節 5.1 至 5.4 之技術規範內容。

安全等級依(1)相關資安風險高低、(2)安全技術實現複雜度，分為 1 級、2 級、3 級三個等級，產品須先通過較低安全等級之測試，始可進行進階等級之測試。

表 1 實機測試總表

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
系統安全	5.1.1 作業系統與網路服務安全測試	-	-	-
	5.1.2 網路服務管控測試	-	-	
	5.1.3 軟韌體版本更新測試	-	-	
	5.1.4 日誌檔與警示測試	-	-	
	5.1.5 安全敏感性資料儲存測試	-	-	
	5.1.6 網頁管理介面安全測試	-	-	-
通訊安全	5.2.1 資料完整性及來源驗證測試	-	-	-
	5.2.2 安全敏感性資料傳輸測試	-	-	-
	5.2.3 傳輸對象限制測試	-	-	-
	5.2.4 Wi-Fi 通訊安全測試	-	-	-
實體安全	5.3.1 實體防護測試	5.3.1.1 5.3.1.2	-	-
	5.3.2 實體介面之安全管控測試	5.3.2.1	-	-
身分鑑別與授權機制安全	5.4.1 身分鑑別測試	5.4.1.1 5.4.1.2	5.4.1.3 5.4.1.4	-
	5.4.2 通行碼設定測試	5.4.2.1	5.4.2.2	-
	5.4.3 權限管控測試	5.4.3.1 5.4.3.2	-	-

5. 資安測試規範

5.1 系統安全測試

檢視廠商書面送審資料是否符合產品系統安全測試執行之測試條件需求，並依下列各測試項目進行實機測試。

5.1.1 作業系統與網路服務測試

5.1.1.1 同 TAICS TS-0021-1。

5.1.2 網路服務管控測試

5.1.2.1 同 TAICS TS-0021-1。

5.1.3 軟韌體版本更新測試

5.1.3.1 同 TAICS TS-0021-1。

5.1.4 日誌檔與警示測試

5.1.4.1 同 TAICS TS-0021-1。

5.1.5 安全敏感性資料儲存測試

5.1.5.1 同 TAICS TS-0021-1。

5.1.6 網頁管理介面安全測試

5.1.6.1 同 TAICS TS-0021-1。

5.2 通訊安全測試

檢視廠商書面送審資料是否符合產品通訊安全測試執行之測試條件需求，並依下列各測試項目進行實機測試。

5.2.1 資料完整性及來源驗證測試

5.2.1.1 同 TAICS TS-0021-1。

5.2.2 安全敏感性資料傳輸測試

5.2.2.1 同 TAICS TS-0021-1。

5.2.3 傳輸對象限制測試

5.2.3.1 同 TAICS TS-0021-1。

5.2.4 Wi-Fi 通訊安全測試

5.2.4.1 同 TAICS TS-0021-1。

5.3 實體安全測試

檢視廠商書面送審資料是否符合產品實體安全測試執行之測試條件需求，並依下列各測試項目進行實機測試。

5.3.1 實體防護測試

5.3.1.1 產品擴充卡插槽防護示警測試

(a) 測試依據：

TAICS TS-0020-2 v2.0「智慧巴士資通訊系統資安標準－第二部：車載機」第 5.3.1.1 節。

(b) 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。

(c) 測試條件：

(1) 產品需提供通知告警方式之書面資料。
(2) 產品外觀無擴充卡插槽，則此測項不適用。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 檢視產品之擴充卡插槽是否具保護措施。
(2) 將擴充卡插槽保護拆解，確認是否可輕易辨識遭拆解(如防拆貼紙破損)或發出通知告警訊息。

(f) 預期結果：

(1) 擴充卡插槽具保護措施。
(2) 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。

5.3.1.2 產品外殼拆解測試

(a) 測試依據：

TAICS TS-0020-2 v2.0「智慧巴士資通訊系統資安標準－第二部：車載機」第5.3.1.2 節。

(b) 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。

(c) 測試條件：

無。

(d) 測試佈局：

無。

(e) 測試方法：

檢視產品外觀是否有防拆機制(例如防拆貼紙、防拆封條...等)，並將產品外殼拆開。

(f) 預期結果：

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。

5.3.2 實體介面之安全管控測試

5.3.2.1 產品實體連接介面安全管控測試

(a) 測試依據：

TAICS TS-0020-2 v2.0「智慧巴士資通訊系統資安標準－第二部：車載機」第5.3.2.1 節。

(b) 測試目的：

驗證是否可透過產品實體連接介面，存取作業系統之除錯模式。

(c) 測試條件：

產品外部不存在實體連接介面則此測項不適用。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 透過實體連接介面(例如：UART、JTAG、USB 等)將測試電腦與產品連線。

(2) 若可以連線，確認是否需身分鑑別方可存取作業系統之除錯模式，且身分鑑別須符合 5.4.2.1、5.4.2.2 之預期結果。

(f) 預期結果：

(1) 無法透過實體連接介面存取產品資料。

(2) 實體連接介面需經身分鑑別方可存取作業系統之除錯模式。

5.4 身分鑑別安全測試

檢視廠商書面送審資料是否符合產品身分鑑別安全測試執行之測試條件需求，並依下列各測試項目進行實機測試。

5.4.1 身分鑑別測試

5.4.1.1 產品實體操作介面測試

(a) 測試依據：

TAICS TS-0020-2 v2.0「智慧巴士資通訊系統資安標準－第二部：車載機」第 5.4.1.1 節。

(b) 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。

(c) 測試條件：

(1) 產品須提供透過實體操作介面進入除錯模式之方法。

(2) 若不存在透過實體操作介面進入除錯模式的功能，則此測項不適用。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 嘗試透過實體操作介面(例如實體按鍵或觸控面板)進入除錯模式。

(2) 檢視是否具身分鑑別機制方可進入除錯模式。

(3) 若身分鑑別機制採用通行碼鑑別，檢視是否依照 5.4.2.1 之安全性要求。

(f) 預期結果：

(1) 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。

(2) 採用的通行碼鑑別機制，符合 5.4.2.1 的要求。

5.4.1.2 身分鑑別錯誤訊息測試

(a) 測試依據：

TAICS TS-0020-2 v2.0「智慧巴士資通訊系統資安標準－第二部：車載機」第5.4.1.2 節。

(b) 測試目的：

驗證身分鑑別錯誤訊息不會造成安全敏感性資料的洩漏。

(c) 測試條件：

此測項對象為網頁管理介面，及透過實體操作介面、實體連接介面(例如：UART、JTAG、USB 等)登入之管理介面，若無該介面則不適用。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 輸入已存在之用戶帳號搭配錯誤的通行碼，檢視鑑別錯誤訊息。

(2) 輸入不存在之用戶帳號，檢視鑑別錯誤訊息。

(f) 預期結果：

從鑑別錯誤訊息無法推斷出合法使用者名稱。

5.4.1.3 鑑別機制強度測試

(a) 測試依據：

TAICS TS-0020-2 v2.0「智慧巴士資通訊系統資安標準－第二部：車載機」第5.4.1.3 節。

(b) 測試目的：

驗證產品網頁管理介面是否具備可靠之身分鑑別機制。

(c) 測試條件：

無。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 將測試電腦連接產品。

(2) 根據產品使用說明，開啟相應之管理介面連接工具。

(3) 執行身分鑑別操作，同時側錄封包，並檢視是否確實執行身分鑑別。

(4) 將側錄到的身分鑑別封包，在另一次身分鑑別操作時，重新發送至受測產品。

(5) 檢視鑑別結果是否成功。

(6) 執行產品登出並再次登入，檢視身分鑑別功能是否正常執行。

(f) 預期結果：

(1) 透過網頁管理介面存取產品時，皆經過身分鑑別程序。

(2) 身分鑑別機制具備抵抗重送攻擊的能力。

(3) 登出後確實須再次登入，方可存取產品。

5.4.1.4 身分鑑別輸入頻率及次數限制測試

(a) 測試依據：

TAICS TS-0020-2 v2.0「智慧巴士資通訊系統資安標準－第二部：車載機」第5.4.1.4 節。

(b) 測試目的：

驗證網頁管理介面之身分鑑別機制是否有防止暴力破解之能力。

(c) 測試條件：

(1) 產品須有網頁管理介面，且該介面須支援身分鑑別機制，否則此測項不適用。

(2) 產品之用戶帳號及通行碼已經建立。

(3) 產品須提供帳戶鎖定機制之設計說明。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 將測試電腦連接產品。

(2) 根據產品使用說明，開啟相應之管理介面連接工具以執行身分鑑別。

(3) 不斷輸入錯誤且相異的通行碼。

(4) 檢視產品於帳戶鎖定計數器重設為 0 前，連續登入失敗次數 5 次以內，是否會鎖定帳戶。

(5) 帳戶鎖定後，於鎖定期間內持續輸入相異且錯誤的通行碼，比對廠商宣告帳戶鎖定時限內，檢視帳戶是否解除鎖定。

(6) 同一帳戶任一次登入失敗後，於廠商宣告計數器重設時限內，重新輸入錯誤且相異的通行碼，檢視輸入失敗次數是否有重新計算。

(f) 預期結果：

(1) 輸入次數 5 次以內，會鎖定帳戶。

(2) 於廠商宣告之帳戶鎖定時限內，帳戶未解除鎖定。

(3) 於廠商宣告計數器重設時限內，失敗次數未重新計算。

5.4.2 通行碼設定測試

5.4.2.1 通行碼長度測試

(a) 測試依據：

TAICS TS-0020-2 v2.0「智慧巴士資通訊系統資安標準－第二部：車載機」第 5.4.2.1 節。

(b) 測試目的：

驗證產品的通行碼長度是否足夠，以確保其強度。

(c) 測試條件：

(1) 此測項對象為網頁管理介面，及透過實體操作介面、實體連接介面(例如：UART、JTAG、USB 等)登入之管理介面，若無該介面則不適用。

(2) 產品須支援通行碼鑑別機制，否則此測項不適用。

(3) 若不存在變更通行碼之功能，則以書面方式審查現有通行碼。

(4) 產品須提供現有之用戶帳號及通行碼。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 將測試電腦連接產品。

(2) 從網頁管理介面或實體操作介面，建立或變更通行碼。

(3) 輸入小於 8 個字元長度之通行碼，檢查通行碼是否能成功建立或變更。

(f) 預期結果：

(1) 現有通行碼長度不小於 8 個字元。

(2) 無法建立或變更小於 8 個字元長度之通行碼。

5.4.2.2 通行碼複雜度測試

(a) 測試依據：

TAICS TS-0020-2 v2.0「智慧巴士資通訊系統資安標準－第二部：車載機」第 5.4.2.2 節。

(b) 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。

(c) 測試條件：

(1) 此測項對象為網頁管理介面，及透過實體操作介面、實體連接介面(例如：UART、JTAG、USB 等)登入之管理介面，若無該介面則不適用。

(2) 產品須支援通行碼鑑別機制，否則此測項不適用。

(3) 若不存在變更通行碼之功能，則以書面方式審查現有通行碼。

(4) 產品須提供現有之用戶帳號及通行碼。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 將測試電腦連接產品。

(2) 從網頁管理介面或操控程式，建立或變更通行碼。

(3) 輸入僅同時含下述四者字元中的一種及二種，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： !、$、#、%)，檢查通行碼是否能成功建立或變更。

(f) 預期結果：

(1) 現有通行碼複雜度強度足夠。

(2) 無法建立或變更成複雜度強度不足之通行碼。

5.4.3 權限管控測試

5.4.3.1 權限管控機制測試

(a) 測試依據：

TAICS TS-0020-2 v2.0「智慧巴士資通訊系統資安標準－第二部：車載機」第 5.4.3.1 節。

(b) 測試目的：

驗證產品資源的存取是否具有權限控管機制。

(c) 測試條件：

(1) 產品之用戶帳號及相關鑑別因子(如通行碼)已經建立，並且存在系統管理者及一般使用者二類帳號。

(2) 產品須提供角色存取權限之宣告。

(3) 此測項對象為網頁管理介面，及透過實體操作介面、實體連接介面(例如：UART、JTAG、USB 等)登入之管理介面，若無該介面則不適用。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 將測試電腦或行動裝置連接產品。

(2) 透過網頁管理介面、實體操作介面或實體連接介面(例如：UART、JTAG、USB 等)，分別以不同角色登入產品。

(3) 存取產品資源，同時檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。

(4) 若為網頁管理介面，嘗試以同一頁面讓不同權限的角色存取。

(f) 預期結果：

(1) 使用者的身分授權與產品自我宣告相符。

(2) 至少擁有二個以上不同權限的角色。

5.4.3.2 權限有效時間測試

(a) 測試依據：

TAICS TS-0020-2 v2.0「智慧巴士資通訊系統資安標準－第二部：車載機」第 5.4.3.2 節。

(b) 測試目的：

驗證產品遠端連線之授權行為是否存在有限的授權時間長度。

(c) 測試條件：

(1) 產品之用戶帳號及相關鑑別因子(如通行碼)已經建立。

(2) 此測項對象為網頁管理介面、遠端操控程式管理介面，若無該介面則不適用。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 將測試電腦或行動裝置連接產品。

(2) 透過網頁管理介面或操控程式登入產品。

(3) 檢視產品之操控程式或網頁管理介面，閒置時限是否存在供管理者設定的操作介面。

(4) 閒置產品直到超過閒置時限值。

(5) 檢視是否需要重新鑑別方可存取產品。

(f) 預期結果：

(1) 產品遠端連線之授權行為，存在閒置時限供管理者設定。

(2) 遠端連線閒置逾時，須經過身分鑑別方可存取產品。

附錄 A
(規定)
產品概述說明(範例)

送測之產品應提供下表供測試實驗室參閱：

表 A.1 產品概述表

製造商	xxx
產 品 名 稱	xxx
廠 牌	xxx
型號	xxx
軟、韌體版本	xxx
通訊介面	WiFi/4G
網路服務 (埠號)	http(443)
傳輸對象 (IP)	SAMBA(8.8.8.x)
產品流量限制	一分鐘 512 bits
日誌存取權限	唯獨/寫入
角色存取權限	管理者：xxx 使用者：xxx
外觀	<圖>

附錄 B
(規定)
產品安全功能說明(範例)

送測之產品應提供下表供測試實驗室參閱：

表B.1 產品安全功能說明表

項　　目	說明	申請者填寫內容
除錯模式	詳述如何進入除錯模式的步驟，或提拱佐證文件。	
系統使用之SIM卡功能	描述系統所使用的SIM卡功能，或提供佐證文件。	
加密演算法	詳細列出產品所使用之加密演算法及其應用。	
安全敏感性資料保存方式	描述產品如何保存安全敏感性資料。	
人機介面操作方式	描述人機介面所有功能如何操作，或提供佐證文件。	
人機介面認證方式	描述人機介面如何做身分鑑別(如需帳密，請於此提供)。	
管理者身分鑑別方式	詳述如何通過管理者身分權限的步驟(如需帳密，請於此附上)。	
實體操作介面使用方式	描述實體操作介面所有功能如何操作，或提供佐證文件。	
產品與後台連結驗證方式	描述產品與後台連結之驗證方式，或提供佐證文件。	

參考資料

無。

版本修改紀錄

版本	時間	摘要
v1.0	2018/11/16	v1.0 出版
v2.0	2019/08/13	v2.0 出版

地　址・台北市中正區重慶南路二段51號8樓之一
電　話・+886-2-23567698
Email・secretariat@taics.org.tw
www.taics.org.tw