TAICS

TAICS TS-0020-2 v2.0 : 2019

智慧巴士資通訊系統資安標準－第二部：車載機v2

Intelligent Bus Telematics System Security Standard - 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標準

-第二部：車載機 v2

Intelligent Bus Telematics System Security Standard

- Part 2: On Board Unit v2

出版日期: 2019/08/13

終審日期: 2019/07/26

誌謝

本標準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

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。

本標準由經濟部工業局支持研究制定。

目錄

誌謝 1
目錄 2
前言 3
引言 4
1. 適用範圍 6
2. 引用標準 7
3. 用語及定義 8
4. 安全等級 9
4.1 安全等級概述 9
5. 標準規範 12
5.1 系統安全要求 12
5.2 通訊安全要求 13
5.3 實體安全要求 14
5.4 身分鑑別與授權機制安全要求 15
附錄 A (參考) 本標準適用範圍之資安脆弱點/要求事項與標準規範對照表 16
參考資料 18
版本修改紀錄 19

前言

本標準係依台灣資通產業標準協會(TAICS)之規定，經理事會審定，由協會公布之產業標準。

本標準並未建議所有安全事項，使用本標準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。

本標準之部分內容，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，並致力於推動資安以及其檢測標準，其中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，目前公車產業已有八成公車(約兩萬兩千輛)轉換為智慧巴士，公車做為交通基礎建設的一部份，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 TAICS TS-0020 智慧巴士資通訊系統資安標準系列(以下簡稱 TAICS TS-0020 系列)之制定，提供產品商或系統服務商在研發產品時有可遵循之安全設計準則，以提升國內智慧巴士資通訊系統相關產品之品質及競爭力。

本文為 TAICS TS-0020 智慧巴士資通訊系統資安標準系列的 TAICS TS-0020-2「智慧巴士資通訊系統資安標準－第二部：車載機」(以下簡稱本標準)，須結合 TAICS TS-0020-1「智慧巴士資通訊系統資安標準－第一部：一般要求」來使用。本標準係以車載機產品為訂定標的，參考「台灣車聯網協會」(Taiwan Telematics Industry Association，以下簡稱 TTIA)「營業大客車車載機產業標準」制定，於「智慧巴士資通訊系統資安標準－第一部：一般要求」中，我們將智慧巴士資通訊系統分為車輛端、路側端及後台端(如圖 1 所示)，藉由彼此間提供的資訊確保車輛端輔助管理、正常運行，達到車輛行車安全。本標準所規範之車載機屬於車輛端，其功能係用以輔助車輛隊管理及監督並輔助駕駛，且須擁有人機操作介面。

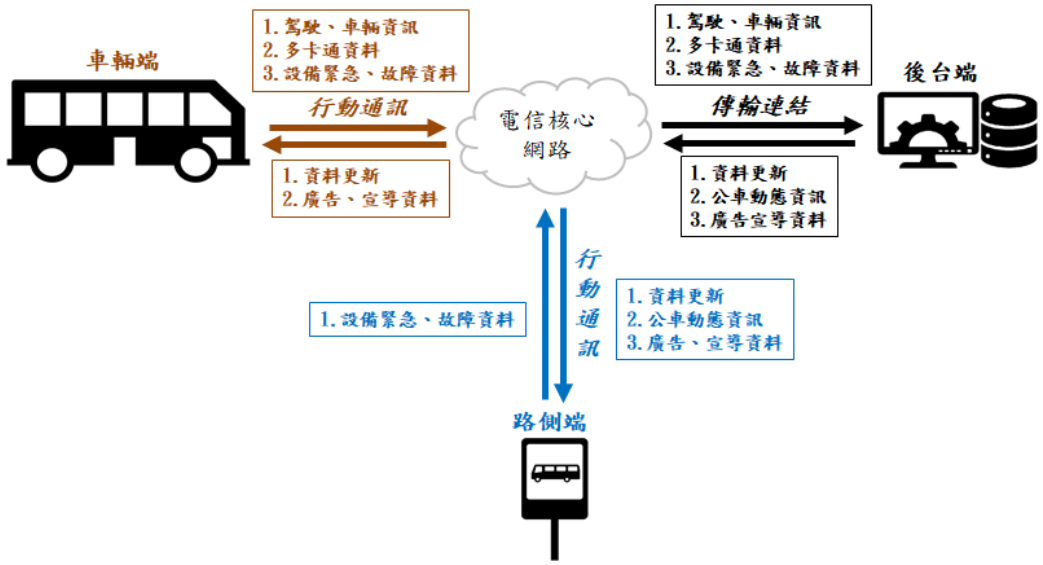

圖 1 智慧巴士資通訊系統架構

本標準參考 TTIA「營業大客車車載機產業標準」及廠商問卷調查結果，對車載機進行相對於 TAICS TS-0020-1「智慧巴士資通訊系統資安標準－第一部：一般要求」之額外資安風險分析，額外風險具有實體盜取、實體破壞、安全敏感性資料之竊取或竄改、錯誤韌體版本更新、實體及遠端惡意控制等風險；本標準制定分為四大構面：系統安全、通訊安全、實體安全及身分鑑別安全。本標準以實體安全、身分鑑別安全避免實體盜取、破壞及實體惡意控制風險；以系統安全避免安全敏感性資料之竊取及錯誤韌體更新；以系統、通訊安全及身分鑑別安全避免遠端惡意控制。

本標準係訂定相對於 TAICS TS-0020-1「智慧巴士資通訊系統資安標準－第一部：一般要求」之額外標準，故車載機產品須遵守 TAICS TS-0020-1「智慧巴士資通訊系統資安標準－第一部：一般要求」及本標準之資安要求。

本系列標準(TS-0020-1、TS-0020-1、TS-0020-2)因應「營業大客車車載機產業標準」v2.0 增訂內容，以及相關業者之需求進行文件改版。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，另對原條文內容進行調整。改版差異請見版本修改紀錄。

1. 適用範圍

本標準依據 TTIA「營業大客車車載機產業標準」v2.0 所界定之產品為範疇，制定資安相關安全要求，其適用範圍為：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。

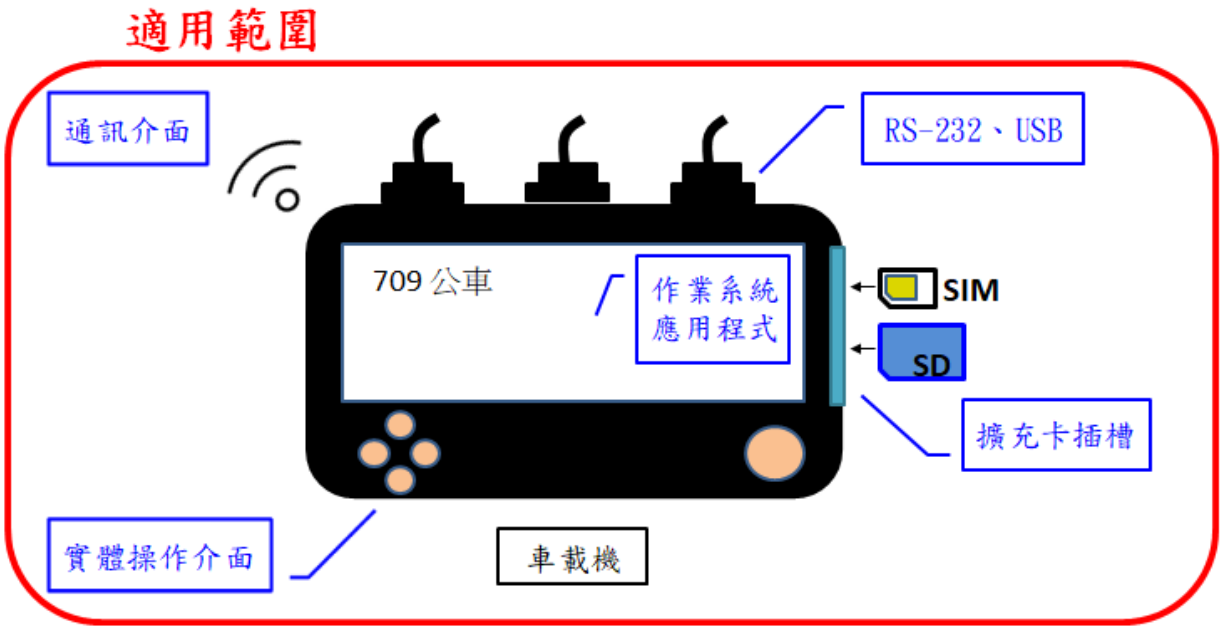

圖 2 適用範圍示意圖

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。

CNS 27001 資訊技術－安全技術－資訊安全管理系統－要求事項

CNS 29100 資訊技術－安全技術－隱私權框架

TAICS TS-0020-1 「智慧巴士資通訊系統資安標準－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-0020-1「智慧巴士資通訊系統資安標準－第一部：一般要求」所述之用語及定義適用於本標準。

4. 安全等級

安全等級係為降低或消弭產品之實體與資訊安全威脅，透過分項檢視，確保產品達到安全之要求。

4.1 安全等級概述

標準安全構面分為：(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，並根據四面向給出分項於安全等級總表，如表 1 所示，第一欄為安全構面；第二欄為安全要求分項，係依各安全構面設計對應之安全要求分項；第三欄為安全等級，按各安全要求分項之驗證結果，作為安全等級評估標準。本安全等級總表各欄的關連性，須依循章節 5.1 至 5.4 之技術規範內容。

表 1 安全等級總表

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	-	-	-
	5.1.2 網路服務管控	-	-	
	5.1.3 軟韌體版本更新	-	-	
	5.1.4 日誌檔與警示	-	-	
	5.1.5 安全敏感性資料儲存	-	-	
	5.1.6 網頁管理介面安全	-	-	-
通訊安全	5.2.1 資料完整性及來源驗證	-	-	-
	5.2.2 安全敏感性資料傳輸	-	-	-
	5.2.3 傳輸對象限制	-	-	-
	5.2.4 Wi-Fi 通訊安全	-	-	-
實體安全	5.3.1 實體防護	5.3.1.1 5.3.1.2	-	-
	5.3.2 實體介面之安全管控	5.3.2.1	-	-
身分鑑別與授權機制安全	5.4.1 身分鑑別	5.4.1.1 5.4.1.2	5.4.1.3 5.4.1.4	-
	5.4.2 通行碼設定	5.4.2.1	5.4.2.2	-
	5.4.3 權限管控	5.4.3.1 5.4.3.2	-	-

4.1.1 安全構面

(a) 系統安全：產品之作業系統、網路服務、版本更新服務及韌體程式設計等須具備足夠安全防護，應視為系統安全要求之標的。

(b) 通訊安全：資料完整性驗證、安全敏感性資料傳輸，和通訊服務是否存在未知之資安漏洞，應視為通訊安全要求之標的。

(c) 實體安全：產品輕易被拆解與否、周邊產品連接驗證，或產品資料儲存與測試用連接埠處置，應視為實體安全要求之標的。

(d) 身分鑑別與授權機制安全：使用者身分鑑別、通行碼設定安全與否，應視為身分鑑別與授權機制安全要求之標的。

4.1.2 安全要求分項

依安全構面所設計對應之安全要求要項，且每一安全要求分項包含一個以上之安全要求。

4.1.3 安全等級

安全等級依(1)相關資安風險高低、(2)技術實現複雜度綜合考量，分為 1 級、2 級、3 級三個等級。其對應之列即其所應符合的安全要求分項，安全等級級數的大小代表安全等級的高低，欲符合較高等級之安全要求必須先滿足較低安全等級要求。

5. 標準規範

本節詳盡載明智慧巴士車載機裝置為滿足資安防護應採取的共通方法，所有智慧巴士車載機裝置應符合本節中所有安全要求。

5.1 系統安全要求

5.1.1 作業系統與網路服務

5.1.1.1 同 TAICS TS-0020-1。

5.1.2 網路服務管控

5.1.2.1 同 TAICS TS-0020-1。

5.1.3 軟韌體版本更新

5.1.3.1 同 TAICS TS-0020-1。

5.1.4 日誌檔與警示

5.1.4.1 同 TAICS TS-0020-1。

5.1.5 安全敏感性資料儲存

5.1.5.1 同 TAICS TS-0020-1。

5.1.6 網頁管理介面安全

5.1.6.1 同 TAICS TS-0020-1。

5.2 通訊安全要求

5.2.1 資料完整性及來源驗證

5.2.1.1 同 TAICS TS-0020-1。

5.2.2 安全敏感性資料傳輸

5.2.2.1 同 TAICS TS-0020-1。

5.2.3 傳輸對象限制

5.2.3.1 同 TAICS TS-0020-1。

5.2.4 Wi-Fi 通訊安全

5.2.4.1 同 TAICS TS-0020-1。

5.3 實體安全要求

5.3.1 實體防護

確認實體產品是否受到保護，如被拆開或破壞時是否能即時發出通知至管理者以及進行識別。

5.3.1.1 產品之擴充卡插槽須進行保護，其保護若遭實體破壞須可輕易識別，或應進行通知管理者，推播警示、告警等訊息。

5.3.1.2 產品外殼需有防拆機制以利辨識產品是否曾遭拆解。

5.3.2 實體介面之安全管控

確認產品實體連接介面是否具權限管控。

5.3.2.1 產品之實體連接介面(例如：UART、JTAG、USB 等)預設須關閉，或須經過身分鑑別方可存取作業系統之除錯模式。

5.4 身分鑑別與授權機制安全要求

5.4.1 身分鑑別

產品使用須具身分鑑別機制。

5.4.1.1 透過產品實體操作介面進入除錯模式前，須進行身分鑑別。

5.4.1.2 身分鑑別失敗顯示的訊息，不得出現可判斷該身分是否存在之資訊。

5.4.1.3 遠端讀存取產品資源前，須透過具備防止重送攻擊之身分鑑別機制。

5.4.1.4 遠端讀存取產品應限制身分鑑別失敗次數，連續五次錯誤即鎖定身分鑑別功能，經一定時間(廠商須定義說明時間長短)後方可將計數器重新歸零並開放身分鑑別。

5.4.2 通行碼設定

確認通行碼強度是否足夠。

5.4.2.1 產品使用者通行碼長度須為 8 個字元以上。

5.4.2.2 除透過實體操作介面登入的情況外，通行碼強度原則參照政府組態基準之通行碼原則類別，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： !、$、#、%)。

5.4.3 權限管控

區分不同使用者所能存取資源的範圍。

5.4.3.1 產品須將使用者角色切割成數個使用者環境，例如：一般使用者與系統管理者等，並於產品文件中定義個別的權限，確保產品之角色權限與產品文件所宣告的相符。

5.4.3.2 產品遠端連線之授權行為，須存在閒置時限供管理者設定，假如遠端連線逾時、遺失或結束，須要求新的鑑別。

附錄 A
(參考)
本標準適用範圍之資安脆弱點/要求事項與標準規範對照表

表 A.1 本標準適用範圍之資安脆弱點/要求事項與標準規範對照表

本標準適用範圍(營業大客車車載機產業標準)	資安脆弱點	本標準要求事項	對應標準規範	
			CNS27001	OWASP 對應項目[1]
3.6.4 智慧駕駛行車應用系統	存取權限管理不當	5.1.7.1	A.9.2.2 使用者存取權限之配置	I2: Insufficient Authentication/Authorization
3.6.4 智慧駕駛行車應用系統	存取權限管理不當	5.1.7.2	A.9.2.2 使用者存取權限之配置	I2: Insufficient Authentication/Authorization
3.6.4 智慧駕駛行車應用系統	存取權限管理不當	5.1.7.3	A.9.2.2 使用者存取權限之配置	I2: Insufficient Authentication/Authorization
3.3 硬體規格	缺乏實體保護機制	5.3.1.1	A.11.2.1 設備安置及保護	I10: Poor Physical Security
-	缺乏實體保護機制	5.3.1.2	A.11.2.1 設備安置及保護	I10: Poor Physical Security
-	缺乏適當之驗證機制	5.3.2.1	A.9.2.2 使用者存取權限之配置	I2: Insufficient Authentication/Authorization
-	缺乏適當之驗證機制	5.4.1.1	A.9.2.2 使用者存取權限之配置	I2: Insufficient Authentication/Authorization
3.6.4 智慧駕駛行車應用系統	缺乏適當之驗證機制	5.4.1.2	A.9.2.2 使用者存取權限之配置	I2: Insufficient Authentication/Authorization
3.6.4 智慧駕駛行車應用系統	缺乏適當之驗證機制	5.4.1.3	A.9.2.2 使用者存取權限之配置	I2: Insufficient Authentication/Authorization
3.6.4 智慧駕駛行車應用系統	缺乏適當之驗證機制	5.4.1.4	A.9.2.2 使用者存取權限之配置	I2: Insufficient Authentication/Authorization
3.6.4 智慧駕駛行車應用系統	通行碼強度不足	5.4.2.1	A.9.4.3 通行碼管理系統	I2: Insufficient Authentication/Authorization
3.6.4 智慧駕駛行車應	通行碼強度	5.4.2.2	A.9.4.3 通行	I2: Insufficient

用系統	不足		碼管理系統	Authentication/Authorization
-	存取權限管理不當	5.4.3.1	A.9.2.2 使用者存取權限之配置	I2: Insufficient Authentication/Authorization
-	存取權限管理不當	5.4.3.2	A.9.2.2 使用者存取權限之配置	I2: Insufficient Authentication/Authorization

參考資料

[1] Open Web Application Security Project (OWASP), Top IoT Vulnerabilities, https://www.owasp.org/index.php/Top_IoT_Vulnerabilities

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