TAICS

TAICS TS-0020-1 v2.0 : 2019

智慧巴士資通訊系統資安標準－第一部：一般要求v2

Intelligent Bus Telematics System Security Standard - Part 1: General Requirements 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

-第一部：一般要求 v2

Intelligent Bus Telematics System Security Standard

- Part 1: General Requirements 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

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。

TAICS TS-0020 系列旨在加強既有智慧巴士資通訊系統之資安防護，故此系列資安標準主要參考「台灣車聯網產業協會」(Taiwan Telematics Industry Association，以下簡稱 TTIA) 所制定之「營業大客車車載機與週邊產業標準」系列，經由與 TTIA 協會、專家學者們共同討論，並參照國際物聯網相關資安標準/規範，如 ISO 26262[1]、ANSI/CAN/UL 2900-1[2]、Groupe Speciale Mobile Association (GSMA) IoT Security Guideline[3]、Open Web Application Security Project (OWASP) Top IoT Vulnerabilities[4]、美國國家公路交通安全管理局的 Cybersecurity Risk Management Framework Applied to Modern Vehicles[5]、Cybersecurity best practices for modern vehicles[6]及日本政府的物聯網安全指導方針[7]等來制定本系列標準。

智慧巴士資通訊系統分為車輛端、路側端及後台端，車輛端包括：車載機、多卡通電子票證、到站顯示系統、數位行車紀錄器模組，路側端包括智慧站牌，後台端架設於各縣市政府係用以接收、處理、傳送資料至車輛端及路側端。一般而言，車輛端係透過車載機與後台端傳輸資料，資料多為行車資訊、多卡通資料、廣告、宣導、設備緊急、故障資料等，藉由上述資訊確保車輛端輔助管理、正常運行，達到車輛行車

安全；路側端與後台端的傳輸資料為公車動態、廣告、宣導資料、設備緊急、故障資料等，資通訊系統架構如圖 1 所示。

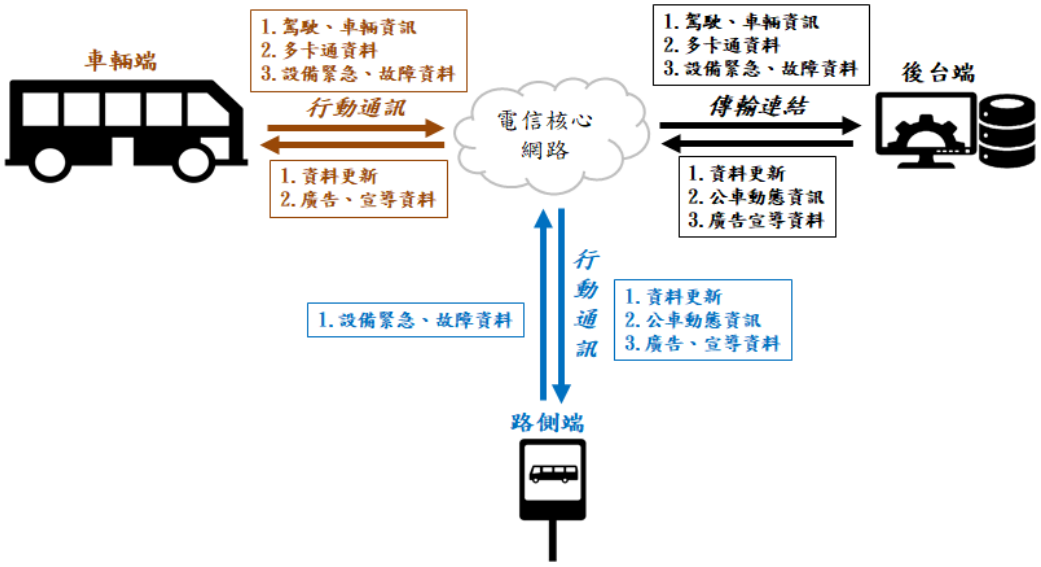

圖 1 智慧巴士資通訊系統架構

因後台端架設時，相關應用系統、伺服器等設備於各單位已有各自之資安規範及要求，故此版系列標準不另制定後台端資安標準。本系列標準範圍針對智慧巴士營運之兩項重要設備：車載機、智慧站牌，共有資安要求項目訂定規範，以補強設備端不足之資安要求；未來亦會配合相關智慧巴士資通訊設備產業標準改版進行滾動修訂。TAICS TS-0020 系列訂定三部標準，包括：「TAICS TS-0020-1「智慧巴士資通訊系統資安標準－第一部：一般要求」(以下簡稱本標準)、「TAICS TS-0020-2「智慧巴士資通訊系統資安標準－第二部：車載機」[8]及「TAICS TS-0020-3「智慧巴士資通訊系統資安標準－第三部：智慧站牌」[9]，本協會亦制定 TAICS TS-0021 系列測試規範，提供測試方法及基準以驗證產品符合 TAICS TS-0020 系列標準。

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 及「營業大客車智慧站牌產業標準」v1.5 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：

(a) 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。

(b) 架設於營業用大客車所行駛營運路線站點，提供到站資訊或即時動態資訊之智慧站牌產品。

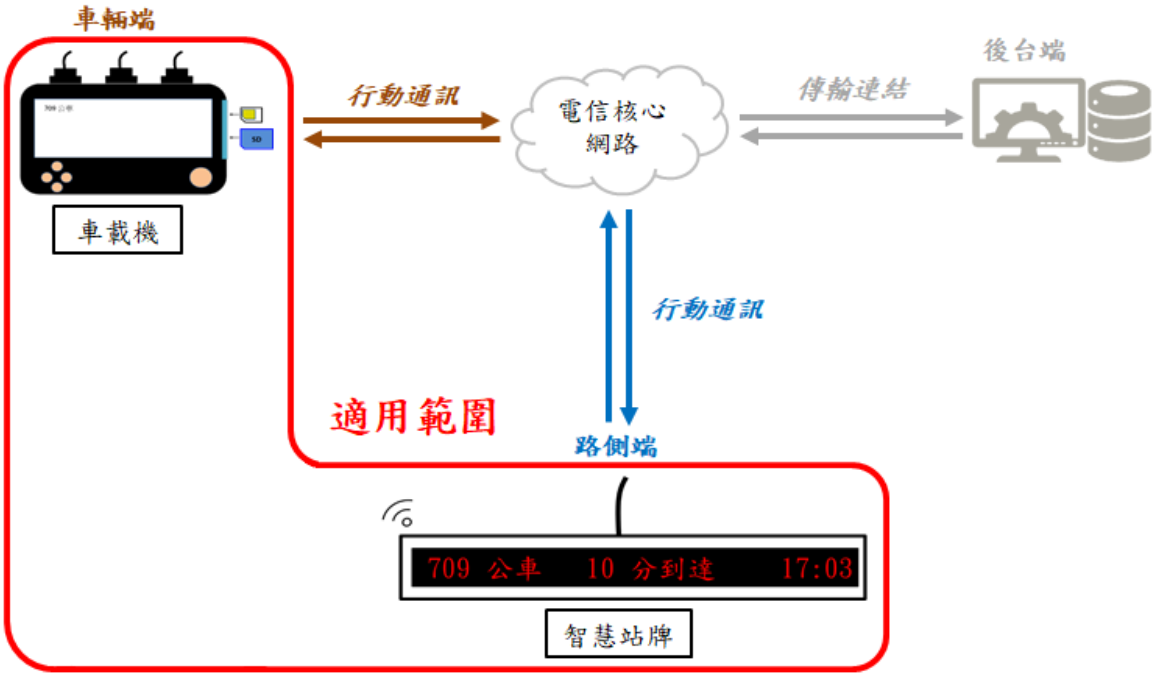

圖 2 適用範圍示意圖

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

台灣車聯網產業協會 「營業大客車車載機產業標準」v2.0

台灣車聯網產業協會 「營業大客車智慧站牌產業標準」v1.5

3. 用語及定義

下列用語及定義適用於本標準。

3.1 車載機 (On Board Unit)

安裝於營業用大客車上，藉由串接車內周邊產品(多卡通讀卡機、到站顯示器、數位行車紀錄器)以提供行車資訊串接、安全輔助、駕駛輔助及車輛管理輔助的功能。

3.2 智慧站牌 (Intelligent Bus Stop)

架設於營業用大客車所行駛營運路線上之站點，提供營業用大客車預估到站資訊或即時動態資訊之產品。

3.3 除錯模式 (Debug Mode)

又稱工程模式(Engineer Mode)，一般於開發或修補階段，產品會處在此模式中。此模式可存取之系統資源不會受限，且還會顯示錯誤訊息提供工程人員除錯用。

3.4 通行碼 (Password)

係指一組能讓使用者使用系統或以識別使用者身分之字元串。

3.5 美國國家弱點資料庫 (National Vulnerabilities Database)

係指美國國家標準技術研究所(National Institute of Standards and Technology, NIST)提供的美國國家弱點資料庫[10]，負責常見弱點與漏洞(如 3.6 所述)之資料的發布及更新。

3.6 常見弱點與漏洞 (Common Vulnerabilities and Exposures, CVE)

簡稱「CVE」，由美國國土安全部贊助之弱點管理計畫，針對每一弱點項目給予全球認可之唯一共通編號。

3.7 通用漏洞評分系統 (Common Vulnerability Scoring System, CVSS)

簡稱「CVSS」[11]，使用 IT 漏洞的特點與影響進行評分，由美國國家基礎建設諮詢委員會負責研究(National Infrastructure Advisory Council, NIAC)，現轉由資安事件應變小組論壇(Forum of Incident Response and Security Teams, FIRST)發展。

3.8 嚴重性等級 (Severity Rating)

係指漏洞評分系統之評比分數，皆有其對應之嚴重性等級，分別是 0 分為無(None)嚴重性、0.1-3.9 分為低(Low)嚴重性、4.0-6.9 分為中(Medium)嚴重性、7.0-8.9 分高(High)嚴重性及 9.0-10.0 為重大(Critical)嚴重性。

3.9 金鑰雜湊訊息鑑別碼 (Keyed-hash Message Authentication Code; KMAC)

又稱為雜湊訊息鑑別碼(Hash-based Message Authentication Code; HMAC[12])，通過使用密碼雜湊函數，同時結合一個金鑰所計算出之加密訊息鑑別碼。目前未被破解之密碼雜湊函數為 SHA256 [13]，建議以此密碼雜湊函數計算金鑰雜湊訊息鑑別碼。

3.10 密碼雜湊函數 (Cryptographic Hash Function)

為雜湊函數的一種，它被定義為一單向函數，亦即無法輕易從函數之輸出值找出其輸入值。目前未被破解之版本為 SHA256，建議使用此密碼雜湊函數。

3.11 安全敏感性資料 (Secure Sensitivity Data)

一般泛指依使用者行為或應用程式之運作，於裝置及其附屬儲存媒介建立、儲存或傳輸之資訊，而該資訊之洩漏有對使用者造成損害之虞，除包括 3.12 定義之個人資料之外，並包含但不限定通行碼、金鑰、視訊、地理位置、行事曆及裝置識別符號等有關個人隱私之資料。本標準之安全敏感性資料定義為通行碼、金鑰、國際行動產品識別碼(International Mobile Equipment Identity, IMEI)與國際行動用戶識別碼(International Mobile Subscriber Identity, IMSI)。

3.12 個人資料 (Personal Data)

主要依「個人資料保護法」[14]上定義之所有得以直接或間接方式識別該個人之資料，包括但不限於自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動、國際行動產品識別碼(International Mobile Equipment Identity, IMEI)、國際行動用戶識別碼(International Mobile Subscriber Identity, IMSI)及其他得以直接或間接方式識別該個人之資料。

3.13 加密 (Encryption)

係指明文資訊透過數學演算法進行改變，增強其加密的強度，使原來的資料不可讀而達到保密之目的。

3.14 Wi-Fi 保護設置 (Wi-Fi Protected Setup, WPS)

由 Wi-Fi 聯盟推出的一個通訊協定，得以簡化使用者在無線安全性方面的設定，假如無線接入點啟動 WPS 模式之後，使用者僅需要在用戶端(Client)按下按鈕便即可連線，無須任何繁複的安全性設定。

3.15 Wi-Fi 保護存取 (Wi-Fi Protected Access, WPA)

用以保護網路通訊安全之加密方式，分成 WPA 與 WPA2 兩個標準，改善有線等效加密(WEP)所存在的網路弱點。WPA 採用 Michael 訊息鑑別碼(Michael Message Authentication Code)與 RC4 (Rivest Cipher 4) 加密演算法；而 WPA2 採用的是 CCMP 訊息鑑別碼 (Counter Mode Cipher Block Chaining Message Authentication Code Protocol) 與 AES(Advanced Encryption Standard)[15]加密演算法。

3.16 異常(Abnormal)

內文所提及之異常定義為產品主要功能如路線偏移、網路未連線。

3.17 事件紀錄 (Event Log)

記錄系統發出包括 3.16 之異常及緊急通報、車輛狀態、安全等事件資料(如附錄 D 所示)。

3.18 管理者(Administrator)

具更改作業系統、控制介面、功能應用程式之權限人員，如設備管理者、後台管理者、維修人員。

3.19 使用者(User)

具讀存取產品資訊、功能操作之權限人員，如資料備份者、產品操作者。

3.20 產品 (Product)

內文所提及之產品係指智慧巴士資通訊系統車輛端之車載機或路側端之智慧站牌。

4. 安全等級

安全等級係為降低或消弭產品之資訊安全威脅，透過最適之安全組合，確保產品達到安全之要求。

4.1 安全等級概述

安全等級總表如表 1 所示，第一欄為安全構面，包括：(1)系統安全、(2)通訊安全；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 5.2 之技術規範內容。

表 1 之安全等級共分為 3 級：1 級適用於裝載 RTOS、Non-OS 之車載機、智慧站牌；2 級適用於裝載 well-known OS(windows、Linux、Android 等)之車載機、智慧站牌，3 級適用於裝載 well-known OS，且應用輔助駕駛操控功能所需之車載機、智慧站牌必須達到的基本安全要求。

本標準僅列出車載機與智慧站牌共通之安全構面要求分項，其餘安全構面要求分項分別列於 TS-0020-2、TS-0020-3 中。

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	-	5.1.1.1 5.1.1.2	-
	5.1.2 網路服務管控	5.1.2.1	-	-
	5.1.3 軟韌體版本更新	5.1.3.1 5.1.3.4	5.1.3.2	5.1.3.3 5.1.3.5
	5.1.4 日誌檔與警示	5.1.4.1 5.1.4.2 5.1.4.3	-	-
	5.1.5 安全敏感性資料儲存	-	5.1.5.1 5.1.5.2	-
	5.1.6 網頁管理介面安全	-	5.1.6.1	-
通訊安全	5.2.1 資料完整性及來源驗證	-	-	5.2.1.1
	5.2.2 安全敏感性資料傳輸	5.2.2.1	-	-
	5.2.3 傳輸對象限制	5.2.3.1	-	-
	5.2.4 Wi-Fi 通訊安全	5.2.4.1 5.2.4.2	5.2.4.3	-

4.1.1 安全構面

(a) 系統安全：產品之作業系統、網路服務、版本更新服務及軟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。

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資通訊系統中的車載機、智慧站牌為滿足資安防護應採取的共通方法，所有車載機與智慧站牌產品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安全

確認軟體/韌體、作業系統之使用版本是否存在已公開之常見弱點與漏洞。

5.1.1.1 作業系統與網路服務，不應存在美國國家弱點資料庫所公開的常見弱點與漏洞資料，及通用漏洞評分系統 CVSS v3 評分為高資安風險之漏洞。

5.1.1.2 應限制未經授權軟體的安裝及執行。

5.1.2 網路服務管控

確認不必要之網路服務連接埠是否開啟。

5.1.2.1 非必要服務所需的網路埠須預設為關閉。

5.1.3 軟韌體版本更新

確認軟韌體版本是否能正確地進行更新以及有更新備援措施。

5.1.3.1 產品須具備韌體更新機制。

5.1.3.2 產品須具備應用程式更新機制，且即使發生更新失敗時，系統能回復正常運作。

5.1.3.3 產品須具備作業系統更新機制，且即使發生更新失敗時，系統能回復正常運作。

5.1.3.4 更新須驗證更新檔的完整性，該完整性驗證功能須採用 FIPS PUB 140-2 Annex A [16]所核可之雜湊(hash)演算法。

5.1.3.5 更新須驗證更新檔的合法性，該合法性驗證功能須採用 FIPS PUB 140-2 Annex A [16]所核可之簽章演算法。

5.1.4 日誌檔與警示

確認系統是否能紀錄所發生之重要事件。

5.1.4.1 事件紀錄須具時間戳記及事件內容。

5.1.4.2 產品之事件日誌檔須具備日誌滾動(log rotate)機制。

5.1.4.3 產品發生異常時，應進行通知管理者或推播警示、告警等訊息。

5.1.5 安全敏感性資料儲存

確認安全敏感性資料的存取是經過權限控管並以加密形式儲存。

5.1.5.1 產品所儲存的安全敏感性資料，須經授權方可存取。

5.1.5.2 產品應加密儲存安全敏感性資料，其加密方式須採用 FIPS PUB 140-2 Annex A 所核可之加密演算法。

5.1.6 網頁管理介面安全

確認網頁介面是否存在已公開之常見漏洞。

5.1.6.1 產品之網頁管理介面不應存在 OWASP web top 10 之 Injection 及 Cross-Site Scripting (XSS)攻擊之漏洞。

5.2 通訊安全要求

5.2.1 資料完整性及來源驗證

確認資料傳輸是否可防止竄改或來源偽造之風險。

5.2.1.1 資料傳輸須透過數位簽章來確保資料的完整性與驗證其來源 (此處資料之定義如附錄 C 所示) 。

5.2.2 安全敏感性資料傳輸

確認安全敏感性資料傳輸過程中是否加密以防止資料暴露或竄改。

5.2.2.1 傳輸安全敏感性資料須加密，加密方式須採用 FIPS PUB 140-2 Annex A 所核可之加密演算法。

5.2.3 傳輸對象限制

確認資料傳輸對象是否有限制。

5.2.3.1 產品資料遠端傳輸時，非廠商宣告之傳輸對象不應進行資料傳輸。

5.2.4 Wi-Fi 通訊安全

確認無線通訊的安全性。

5.2.4.1 產品須提供使用者得自行開/關「Wi-Fi 保護設置 (WPS)」之 WPS PIN 功能，而其預設值須為關閉狀態。

5.2.4.2 Wi-Fi 網路之 Wi-Fi 保護存取設置需支援 v2 同等或以上之版本。

5.2.4.3 產品支援 Wi-Fi 協定，則不應存在錯誤處理漏洞，包括檢視訊息長度、訊息識別碼及關鍵協定屬性等欄位，導致產品因發生崩潰而服務中止的情形。

附錄 A
(參考)
資安脆弱點、資安威脅、風險等級及相關構面對應表

表 A.1 資安脆弱點、資安威脅、風險等級及相關構面對應表

資安脆弱點	資安威脅	受影響資產	風險等級	受影響的安全構面			
				系統安全	通訊安全	實體安全	身分鑑別安全
系統具已知安全漏洞	殭屍網路病毒感染、駭客入侵	核心系統軟體	高	O	-	-	O
資料以明碼傳輸	安全敏感性資料遭竊聽	資料傳輸(訊息回覆、資訊回報與緊急通報)	高	O	O	-	-
缺乏資料傳輸完整性及來源驗證	傳輸資料遭竄改	資料傳輸(訊息回覆、資訊回報與緊急通報)	中	-	O	-	O
缺乏適當之存取控制機制	駭客提權	權限控管	中	-	-	-	O

資安脆弱點	資安威脅	受影響資產	風險等級	受影響的安全構面			
				系統安全	通訊安全	實體安全	身分鑑別安全
缺乏完整事件紀錄	發生異常不易偵測	系統事件日誌	中	O	-	-	-
缺乏實體保護機制	惡意實體破壞	實體控制介面、輸出入埠連接、LED 看板顯示	中	-	-	O	-

附錄 B
(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 B.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 (TTIA 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[4]
3.2 系統模組(車載機) -	系統具已知安全漏洞	5.1.1.1	A.12.6.1 技術脆弱性管理	I9: Insecure Software/Firmware
3.2 系統模組(車載機) -	未限制軟體的下載及使用	5.1.1.2	A.12.6.2 對軟體安裝之限制	I9: Insecure Software/Firmware
3.5 通訊協定(車載機) 3.4 通訊協定(智慧站牌)	非服務所需的網路埠未關閉	5.1.2.1	A.13.1.1 網路控制措施	I3: Insecure Network Services
-	韌體版本過舊存在已知漏洞	5.1.3.1	A.12.5.1 對運作中系統之軟體安裝	I9: Insecure Software/Firmware
-	應用程式版本過舊存在已知漏洞、缺乏系統回復機制	5.1.3.2	A.12.5.1 對運作中系統之軟體安裝	I9: Insecure Software/Firmware
-	系統版本過舊存在已知漏洞、缺乏系統回復機制	5.1.3.3	A.12.5.1 對運作中系統之軟體安裝	I9: Insecure Software/Firmware
-	更新檔未驗證	5.1.3.4	A.12.5.1 對運作中系統之軟體安裝	I9: Insecure Software/Firmware
-	更新檔未驗證	5.1.3.5	A.12.5.1 對運作中系統之軟體安裝	I9: Insecure Software/Firmware
3.1 功能需求(車載機) 3.4.2.5 異常回報程序 (智慧站牌)	缺乏完整事件紀錄	5.1.4.1	A.12.4.1 事件存錄	-
-	缺乏日誌完整性	5.1.4.2	A.12.4.1 事件存錄	-
3.5.8.障礙回報程序(車	缺乏異常告警	5.1.4.3	A.16.1.2 通報	-

載機) 3.4.2.5.異常回報程序(智慧站牌)	機制		資訊安全事件	
-	存取權限管理不當	5.1.5.1	A.9.2.2 使用者存取權限之配置	I2: Insufficient Authentication/Authorization
-	缺乏敏感性資料保護機制	5.1.5.2	A.10.1.1 使用密碼式控制措施之政策	I5:Privacy Concerns
3.6.4 智慧駕駛行車應用系統(車載機)	Web 介面具已知安全漏洞	5.1.6.1	A.12.6.1 技術脆弱性管理	I9: Insecure Software/Firmware
3.5.2 訊息內容(車載機) 3.4.2 訊息內容(智慧站牌)	缺乏資料傳輸完整性及來源驗證	5.2.1.1	A.13.2.2 資訊傳送協議	I4: Lack of Transport Encryption
3.5.2 訊息內容(車載機) 3.4.2 訊息內容(智慧站牌)	資料以明碼傳輸	5.2.2.1	A.13.2.4 機密性及保密協議	I4: Lack of Transport Encryption
3.5 通訊協定(車載機) 3.4 通訊協定(智慧站牌)	缺乏適當的網路政策	5.2.3.1	A.13.2.1 資訊傳送政策及程序	I8: Insufficient Security Configurability
3.2 系統模組(車載機) 3.3 通訊技術(智慧站牌)	系統設定不當	5.2.4.1	A.13.1.1 網路控制措施	I8: Insufficient Security Configurability
3.4 通訊技術(車載機) 3.3 通訊技術(智慧站牌)	系統設定不當	5.2.4.2	A.13.1.1 網路控制措施	I8: Insufficient Security Configurability
3.4 通訊技術(車載機) 3.3 通訊技術(智慧站牌)	系統設定不當	5.2.4.3	A.13.1.1 網路控制措施	I8: Insufficient Security Configurability

附錄 C
(參考)
運研所 97 年度公車動態資訊系統交換格式

表 C.1 運研所 97 年度公車動態資訊系統交換格式：控制中心-車機通訊伺服器

分類	功能
行車資訊	定時資料回傳
	定點資料回傳
訊息傳遞	公告訊息下載(供車內 LED 顯示)
	司機訊息下載(供駕駛座前顯示)
	車輛平衡間距訊息下載
	車機異常訊息通報
	通報各車輛之行車狀況(已排未發)
	通報各車輛之行車狀況(未排已發)
基本參數設定	路線名稱設定
	路線站牌設定
	站牌資料設定
班表設定	班表下載
	班表清除
	手動請求班表下載
訊息確認	下載訊息確認回報

表 C.2 運研所 97 年度公車動態資訊系統交換格式：控制中心-站牌通訊伺服器

分類	功能
基本參數設定與查詢	站牌資料查詢
	站牌資料設定
訊息傳遞	更新站牌即時公車資訊
	更新站牌文字資訊
	站牌異常狀況回報
訊息確認	下載訊息確認回報

附錄 D
(參考)
營業大客車車載機產業標準：事件表

表 D.1 營業大客車車載機產業標準：事件表

事件名稱	說明
進出站(圓形偵測)	進出站回報
超轉超速	瞬時轉速超過特定值
	瞬時時速超過特定值
急加/減速	單位時間加速/減速超過限制速度範圍
行駛中前門/後門開啟	前門信號為 1 且速度>0 後門信號為 1 且速度>0
車輛異常回報	停車不熄火（轉速不為 0 且速度為 0 的時間超過特定範圍）
	異常移動（轉速為 0 速度大於 0）
車輛狀態	司機由螢幕改變車輛狀態（包含緊急事件）
異常發車	後端回覆「無班表」，且司機沒有選擇特殊狀態（狀態停留在"未知"），以及車輛已移動特定距離
司機回覆	司機回覆提示訊息
進出特定區域	進出特定區域回報，用於禁止遊覽車行駛之特定區域偵測（此一特定區域相關資訊須由中控中心事前提供車機載入判斷）
路線外營運	車輛進入非核定許可之經營路線（此一路線外營運相關資訊須由中控中心事前提供車機載入判斷）

參考資料

[1] ISO 26262「道路車輛功能安全」

[2] ANSI/CAN/UL 2900-1:2017 Software Cybersecurity for Network Connectable Products, Part 1: General Requirements

[3] Groupe Speciale Mobile Association (GSMA) corp., IoT Security Guidelines for Endpoint Ecosystems.

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

[5] National Highway Traffic Safety Administration (NHTSA), National Institute of Standards and Technology Cybersecurity Risk Management Framework Applied to Modern Vehicles, October 30, 2014.

[6] National Highway Traffic Safety Administration (NHTSA), Cybersecurity best practices for modern vehicles, October, 2016.

[7] 總務省, 經濟產業省, IoT セキュリティガイドライン ver 1.0

[8] 台灣資通產業標準協會，TAICS TS-0020-2 「智慧巴士資通訊系統資安標準－第二部：車載機」

[9] 台灣資通產業標準協會，TAICS TS-0020-3 「智慧巴士資通訊系統資安標準－第三部：智慧站牌」

[10] National Institute of Standards and Technology (NIST), National Vulnerability Database, https://nvd.nist.gov/vuln/full-listing

[11] First, Common Vulnerability Scoring System v3.0 Specification, https://www.first.org/cvss/specification-document

[12] IETF RFC 2104 (1997), HMAC Keyed-Hashing for Message Authentication.

[13] IETF RFC 4634 (2006), US Secure Hash Algorithms (SHA and HMAC-SHA).

[14] 個人資料保護法, Dec., 2015.

[15] National Institute of Standards and Technology (NIST), "Announcing the Advanced Encryption Standard (AES)", October 2, 2012.

[16] National Institute of Standards and Technology (NIST), Annex A: Approved Security Functions for FIPS PUB 140-2: Security Requirements for Cryptographic Modules, May 10, 2017.

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