智慧運輸系統資安威脅與因應
－以車聯網安全為例

Cybersecurity Threats and Responses for Intelligent Transportation Systems
- A Case Study on Internet of Vehicles Security

運輸資訊組　吳東凌 童志浩

研究期間111年2月至111年12月

摘　要

因應物聯網的興起促使汽車產業有了突破性的革新，結合行動互聯網及「智慧運輸系統(ITS)」的協同發展，造就了車聯網產業鏈的創新趨勢。ITS的發展過程中，透過越來越多的網路連結，導致個人資訊、金流交易、行車紀錄軌跡等資訊曝露，增加了網路攻擊的威脅風險。本研究將以車聯網為例，針對支付、管理、通訊三大應用與系統類別可能面臨的資安威脅提出適切可行的防護建議及因應方案，藉此降低或防止可能面臨的攻擊風險與系統安全漏洞，並做為政府部門與民間企業推展車聯網以及消費者對智慧運輸、車聯網之選用參據。

關鍵詞：
資安威脅、車聯網

一、緒論

(一)緣起與研究目的

「科技始終來自於人性」，所有技術的運用最終都要回歸真實生活的需求。觀察近年電子、資訊、通訊與網路等產業的發展，已帶給這個世界巨大的改變與方便，智慧城市、智慧雲端、智慧交通更成為了我們生活中的一部分，而因應新興科技及物聯網的觀念亦促使汽車產業有了突破性的革新，結合行動互聯網及「智慧運輸系統(Intelligent Transport System, 以下簡稱 ITS)」的協同發展，造就了車聯網產業鏈的創新趨勢。

今日的交通運輸系統不僅僅是一項移動工具，更是能協助我們解決交通管理、資源分配的問題，而建構安全且高效率的 ITS 亦是智慧城市發展中不可或缺的項目之一，其中具有聯網及智慧功能的車輛便是重要關鍵。根據研究機構 Counterpoint 預測，至 2022 年內建聯網能力的車輛將成長 270% [1]，這還不包含已經導入網路並可連接使用者物聯網(IoT)裝置的車輛，正因為使用者對 ITS 的持續關注、5G 行動通訊技術衍生的契機以及汽車相關產業(如保險業與 OEM 製造業)的其他商機，都被視為促進 ITS 普及的誘因。也是因為 ITS 所帶來的巨大商業發展，聯網汽車的資安議題也逐漸受到重視，在 ITS 的發展過程中，透過越來越多的網路聯結，導致個人資訊、金流交易及行車紀錄軌跡等資訊曝露，因此也增加了網路攻擊的威脅風險，小至一般駭客入侵，大至國家社會安全威脅與財務損失。

安全(Safety)一直是汽車工業發展過程中不可或缺的一部分，這個概念已在整個供應鏈中理解並實施多年。但是，隨著汽車聯網和自動駕駛等技術的日益發展，這也帶來了新的威脅，新開發的汽車將具備越來越多的外部介面，例如:藍牙(Bluetooth)、Wi-Fi、GSM 或 USB。這些外部介面將讓汽車暴露在網路攻擊的風險下，如果這些外部介面受到攻擊，不僅會造成嚴重的財產損失，亦會帶給乘客極大的傷害。據市場研究機構統計數據指出，2009 年至 2019 年全球針對聯網汽車成功發動的網路攻擊事件，數量就成長了 6 倍，預期未來更會以每年平均 95%的成長率持續增加 [2]，試想假如聯網汽車在交通尖峰時間遭駭客入侵，是有可能導致如同美國 911 恐怖攻擊之規模的意外事件，此時無可避免地將帶來生命財產損失，並造成基礎架構損害。鑑此，著眼於聯網汽車的網路攻擊防範及確保人身安全的重要性，以車輛網路安全為主的 ISO/SAE 21434 標準也應運而生，甚至自 2022 年 7 月起成為歐盟(EU)的強制性規範，要求所有新上市車款必須通過該標準的認證，以防範所有對車輛安全的危害。

(二)研究範圍與對象以及利害關係人

從 ITS 框架來看，ITS 生態系需整合數個不同產業、元件與營運系統才能順利運作，但只要其中一個環節遭到威脅或攻擊，就可能波及其他相關產業，例如：從實體、網路或無線通訊層面的攻擊，因此，保護 ITS 的需求相對增加和網路安全的概念應用於多個領域，考慮到這些攻擊可能造成的損害，制定強而有力的保護措施就變得非常重要，這些措施可以解決系統的漏洞、克服對系統的外部威脅並降低 ITS 可能面臨的攻擊風險。根據蒐集相關文獻的綜述，這些技術在個人車輛中的安全性以及用於公共交通系統的技術變得越來越重要[3-8]，以下我們針對 ITS 架構中六個主要類別在資訊技術應用的項目概略說明：

1. 車輛管理：

   以無線區域網路 (WLAN)及 5G 通訊技術來連接其他內部或外部 IoT 裝置，提供用路人車內、外的即時訊息，實現自動導航並感應周遭環境;在大眾運輸系統方面，藉由攝影機、光學雷達(LIDAR)及 GPS 感應定位系統協助，讓乘客和行控中心都能掌握即時的車輛運輸或行進狀態。

2. 路況回報：

   透過攝影機、偵測系統、道路氣象站及各種感測器，導入道路現況、道路壅塞資訊、車輛事件警告、弱勢行人警告、路況預警等功能，將資料即時傳送至中央監控中心，達到流量與路況即時監控，提升車流效率。

3. 車流控管：

   ITS 導入交通號誌控制系統、鐵路柵欄、動態訊息號誌以及自動化收費系統，來達成即時車流資料蒐集與道路監控，讓行控中心依實際的狀況調整號誌的變換及時間的長短，降低道路壅塞的狀況發生。

4. 支付應用與系統：

   採取自動收費、電腦輔助管理、車輛進出自動辨識系統等，例如：RFID 支付、QR Code 掃描折扣、電子票證等，藉此提高收入並降低其他運營相關成本。

5. 管理應用與系統：

   負責管理各種功能偕同運作的中央系統，可監控車流或定義各種複雜的總量限制，提供一定的控管能力來滿足流量管理中心、停車系統、水陸空運廠商管理、營造與維修中心、緊急服務中心、旅遊資訊及大眾運輸系統等需求。

6. 通訊應用與系統：

資訊交換是 ITS 生態系統的核心，所有營運中心和裝置都要彼此交換資料來共同確保交通流量的效率與安全，並且提高營收、減輕環境衝擊，這其中包含了：車對車(V2V)、車對基礎架構(V2I)、基礎架構對基礎架構(I2I)資訊交換，以及各種工具、媒體與系統，例如：應用程式、社群媒體、網站、警示通知及公告等。

綜上所述，本研究將以車聯網為例，針對支付、管理、通訊三大應用與系統類別可能面臨的資安威脅提出適切可行的防護建議及因應方案，藉此降低或防止可能面臨的攻擊風險與系統安全漏洞，並做為政府部門與民間企業推展車聯網以及消費者對智慧運輸、車聯網之選用參據。

二、文獻探討

(一)ISO/SAE 21434：2021道路車輛－網路安全工程

ISO/SAE 21434:2021，全名是:「道路車輛－網路安全工程 2021 年版」，主要由國際標準組織（ISO）以及國際汽車工程協會（SAE）於 2021 年 8 月 31 日發布，它是一項提供道路車輛產業上、中、下游業者風險管理的標準。範圍涵蓋車輛產品所需之電子、電機系統及其元件、介面在概念、研發、製造、營運、維護和除役等各階段需要考量和監控之資通訊安全風險管理要求，適用對象為道路車輛產業業者及其供應鏈廠商。

本項標準的管理架構和精神引用自 ISO 的各項管理系統，涵蓋資訊安全管理系統 ISO 27001、風險管理系統 ISO 31000、品質管理系統 ISO 9001 和道路車輛功能安全 ISO 26262 等之相關要求，從管理系統的整體思維、風險管理的方法、專案管理的注意項、客戶的溝通和供應商管理，來落實道路車輛在資通訊安全風險的管控。

具體而言，這份標準共有 15 個章節(表 1)以及附錄 A 到附錄 H，所規範的網路安全風險管理工程要求，涵蓋道路車輛的 E/E 系統概念、產品開發、生產、操作、維護與除役報廢。這項標準另一個重要的核心，就是針對威脅分析與風險評估方法提出說明，目標是要讓車輛在早期的產品設計開發時，識別潛在的威脅與安全漏洞。同時，這裡也定義了一個框架，涵蓋網路安全流程的要求，並建立溝通與網路安全風險管理的共通語言。

表 1：ISO/SAE 21434 條文摘要

綱要	對應條款
網路安全管理	§5 包括組織的網絡安全政策、規則和流程的實施，進行整體網絡安全管理
專案相關網路安全管理	§6 專案相關的網絡安全管理
繼續的網絡安全活動	§7 定義活動，該活動為正在進行的風險評估和 E/E 系統的漏洞管理提供資訊，直至支援終止
風險評估方法	§8 定義了確定網絡安全風險程度的方法
概念階段	§9 定義項目和相關資產，確定了網絡安全風險，並定義了網絡安全目標
開發階段	§10 定義網絡安全規範，實現並驗證了特定於項目或組件的網絡安全要求
驗證階段	§11 描述了在車輛等級上某項的網絡安全驗證
生產階段	§12 規定了與項目或組件的製造，組裝或校準有關的網絡安全方面
營運及維護	§13 規定了與網絡安全事件回應，和對項目或組件的更新有關的活動
汰舊/服務終止	§14 包括與項目或組件退役有關的網絡安全注意事項
供應鏈管理	§15 包括對供應商管理的要求

資料來源：本研究整理

簡而言之，推動這項標準的目的，就是為了確保現代的汽車產業，從設計開發、生產到生產後的整個生命周期，都應具有安全設計，重視風險管理，並能涵蓋到整個供應鏈。長期來看，在各國的汽車網路安全規範之外，ISO/SAE 21434 正式發布後，這項標準將是車聯網發展的重要里程碑，畢竟，若缺乏 Security 方面的標準，汽車製造商也難以實現 Safety。相反地，對於全球汽車製造商與供應鏈而言，能在風險管理上，藉此標準來獲得最佳實踐的工具。換言之，在這套國際標準制定之後，也將意謂著，汽車製造商與零組件供應商依循 ISO/SAE 21434 標準，便可符合全球汽車網路安全管理法規要求。

(二)TISAX 汽車安全評估訊息交換

TISAX 係由德國汽車工業協會 (VDA) 根據 ISO 27001 的標準規範所制訂並推出的資訊安全評估 (ISA) 結果平台，確保汽車製造商、服務提

供商和供應商之間的資訊安全統一標準(資料蒐集、資料儲存及資料處理)，並藉由確保製造過程及車輛運作的完整性及可用性來協助保護數據，以提供交換汽車產業的資訊安全評估與審核結果，透過一次評估與多方資訊共享的機制，為汽車製造商和供應商提供了長達三年的安全驗證，且每個登錄參與並通過 TISAX 的企業組織可自行授權合作夥伴以共享 TISAX 上的評估結果，藉此讓汽車供應鏈合作夥伴瞭解其在資訊安全及資料保護上的成果。

(三)ASPICE 汽車產業軟體流程改進與能力測定標準

ASPICE 全稱是“Automotive Software Process Improvement and Capacity Determination”，即汽車軟體過程改進及能力評定，是汽車行業用於評價軟體發展團隊的研發能力水準的模型框架，也是國際標準組織（ISO）和國際電子電機委員會（IEC）的聯合標準之一。

ASPICE 是一項適用於汽車產業評估並持續改善軟體及其相關元件，引用 ISO 33020 和 ISO/IEC 15504 軟體流程評估方式，用來提升軟體、車用的電子控制單元(ECU)/車載電腦的品質，在研發階段監控與管理相關流程之標準。可使開發產品在整個研發生命周期考量並落實品質、功能安全和資通訊安全的管控。其架構可適用於傳統和敏捷式 (Agile) 開發方法且支援關鍵產品工程。在汽車產業，ASPICE 逐漸成為廣泛適用標準，全球各大車商 (Audit、BMW、Ford…) 開始對於其電子零件和軟體供應鏈要求通過 ASPICE 評估

(四)聯合國車輛網路安全管理系統（Cyber Security Management System, CSMS）」

「網路安全管理系統（Cyber Security Management System, CSMS）」於 2021 年 1 月 22 日生效，CSMS 重點在於車輛整體生產流程，包含從設計、製造乃至停產等階段所採行之網路安全管理措施，並詳細羅列車輛網路安全可能之弱點、威脅和攻擊手法，製造商必須根據列表一一擬定因應措施，如建立登入權限分級管理機制或資料與密碼之保護措施等，針對 CSMS 之法規要求我們可以區分為 4 項重點，內容概述詳如表 2：

表 2-網路安全管理系統（CSMS）法規要求重點

區分		內容概述
1	一般性規格	描述本法規不應限制其他聯合國法規的規定或要求。
2	CSMS 相關需求	CSMS 應包含的以下階段： a) 開發階段(development phases) b) 生產階段(production phase) c) 生產後階段(post-production phases) 流程：網絡安全管理 流程：識別車輛風險 流程：風險評鑑、分類和處置 流程：驗證所識別風險被適當管理 流程：測試車輛類型的網絡安全 流程：確保風險評鑑(即第 4 個流程)是最新的 流程：監控、偵測和響應(車輛類型)網絡攻擊、網絡威脅和弱點，確保監控、偵測的持續性，包含： a) 車輛初次被註冊在監控中 b) 從車輛資料和日誌中分析及偵測網絡威脅、弱點、攻擊的能力 (該能力應尊重本法規(法規章節 1.3)，本法規應尊重及車輛擁有者、駕駛人的隱私權，及其意願) 流程：當新網絡威脅與弱點被識別時，應評鑑既有的控制措施，並確保其是否持續有效 流程：提供相關資料以協助分析嘗試性或已成功的網絡攻擊
3	車輛類型需求	應擁有與所批准車輛類型相關的 CSMS 有效合規證明。 應針對批准的車輛類型，識別和管理供應商相關的風險 應針對車輛類型的關鍵(重要)元件，進行更仔細的風險評鑑，並針對所發現的風險進行適當的處置與管理。其中，風險評鑑時應考慮車輛類型的個別單元及其互動，更應進一步考慮與外部系統之間的互動。在進行風險評鑑時，應考慮 Annex 5-Part A 及

區分		內容概述
		其他相關風險。 應因應風險評鑑所識別的風險，保護車輛類型。應採取相稱的緩解措施來保護車輛類型。其中，實施的緩解措施應包括 Annex 5-Part B 和 PartC 中提及的與所識別的風險相關的所有緩解措施。然而，如果 Annex 5-Part B 和 PartC 中提及的緩解措施與所識別的風險沒有關聯，則應確保其他適當的緩解措施被實施。 應採取適當和相稱的措施以確保車輛類型上用於存儲和執行售後軟體、服務、應用程式或數據的專用環境(如果提供)。 在車輛類型認可前，應進行適當和充分的測試，以驗證所實施安全措施的有效性。 應對車輛類型採取措施： a) 偵測和防止對車輛類型的車輛進行網絡攻擊 b) 支持在偵測與車輛類型相關的威脅、漏洞和網絡攻擊方面的監控能力 c) 提供數位鑑識能力，以分析嘗試性或已成功的網絡攻擊 用於本法規的密碼模組應符合共識標準，如果所使用的密碼模組不符合共識標準，則應說明其使用理由。
4	報告規定	車輛製造商應回報給國家技術服務(National technical services) 或認證機構 (Homologation authorities)至少一年一次(或多次，或相關事件)。回報上述流程 8 的監控、偵測和響應的資訊；及上述流程 4 的風險緩解措施資訊 相關內容包含： a)網絡攻擊、網絡威脅和弱點 b)尤其應回報「新網絡攻擊」的相關資訊 c) 相關緩解措施是否持續有效，以及是否有採取的行動 國家技術服務(National technical services)或認證機

區分		內容概述
		構(Homologation authorities)應驗證車輛製造商所提交的資料，如果必要，將會要求車輛製造商補救被認定無效的措施 如果車輛製造商所提交的報告或回應是不足夠的，認證機構可決議撤銷其 CSMS。

資料來源：本研究整理

(五)聯合國車輛軟體更新管理系統（Software Update Management System, SUMS）」

SUMS 規範同樣於 2021 年 1 月 22 日生效，它要求了車廠遵守車輛軟體更新相關程序的義務，包含於發送更新前執行軟硬體兼容性驗證、確保更新不會影響行車安全、充分告知車輛使用人更新內容及更新是否成功，並且利用車型使用系統識別碼（RX Software Identification Number, RXSWIN）機制，完整保存該車型每次更新之軟硬體組態紀錄。

小結：在電動車、自駕車等技術發展之下，車聯網也同時成為必然的趨勢，這也使得汽車需顧慮新的受攻擊面，其資安風險議題也如物聯網技術發展，備受各界關注。依據聯合國歐洲經濟委員會（UNECE）提出「網路安全管理系統（CSMS）」及「軟體更新管理系統（SUMS）」二項標準及要求，未來新車要進行型式認可時，均需要通過 ISO 21434 道路車輛－網路安全工程。透過 ISO 21434，可建立相對完善的管理系統體系，讓供應鏈中的彼此了解在汽車運作的生態系擔任的角色及肩負的責任，以抵禦越來越大的資訊安全風險，製造商必須將同時重點市場開拓與產品安全，並創建一個組織化的網路安全環境，以開發安全的產品。

三、研究方法

為使研究具有系統化、合理化的程序，本研究以預期研究的範圍為核心，蒐集車聯網相關的資安國際標準規範、期刊報導及研究，並整理各標準相對應的條文實施分析，藉此提出相對適合本研究主題之安全控制措施建議(研究流程如圖 1)。

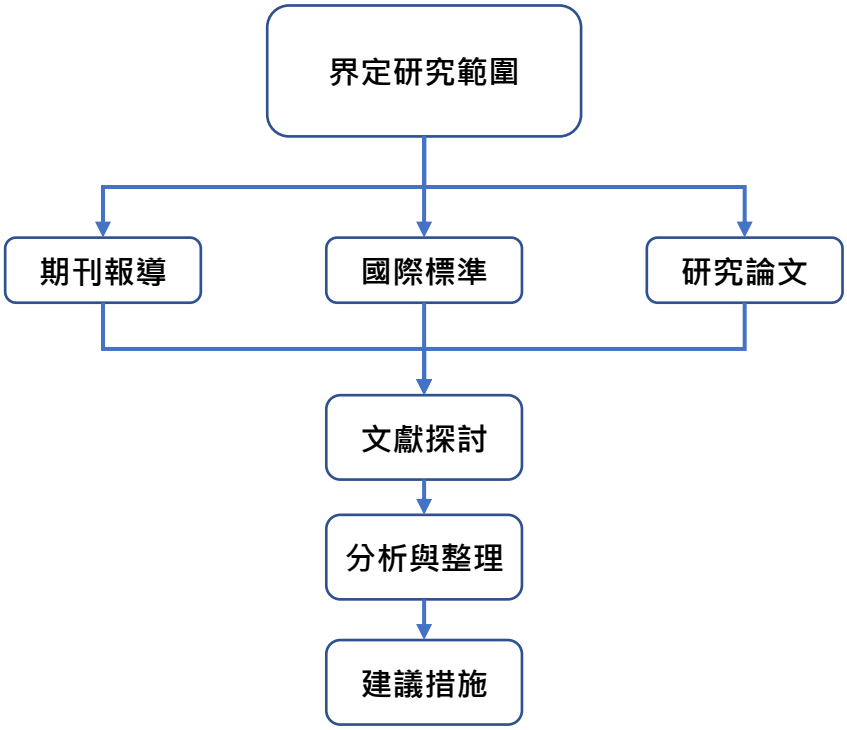

圖 1. 研究流程

四、研究分析與結果

(一)威脅分析

聯網汽車與相關技術的不斷演進，開啟不少提升汽車效率和安全的契機，但隨著 5G 行動通訊技術的發展，致使聯網汽車越來越仰賴 5G，然而網絡犯罪集團也同樣虎視眈眈的開發各種新式攻擊手法，讓聯網汽車與相關技術陷入資安風險中，例如：阻斷服務攻擊(DDoS)、中間人攻擊(MITM)、服務遭到挾持、延遲問題、資料隱私外洩、資料錯誤、組態設定錯誤、雲端供應鏈問題及認證與管理問題。為避免前述外部攻擊風險，在 WP29 的「軟體更新管理系統（SUMS）」規範中，也特別要求車廠遵守車輛軟體更新相關程序義務，包含於發送更新前執行軟硬體兼容性驗證、確保更新不會影響行車安全、充分告知車輛使用人更新內容及更新是否成功，並且利用車型使用系統識別碼（RX Software Identification Number, RXSWIN）機

制，完整保存該車型每次更新之軟硬體組態紀錄 [9]。

此外，歐盟網路安全局（European Union Agency For Cybersecurity, ENISA）於 2019 年 11 月 25 日提出「智慧車輛最佳實務安全準則（Good Practices For Security of Smart Cars）」，亦提供了汽車產業、相關零組件供應商與售後市場服務供應商相關網路安全實務準則，並指出在安全措施與最佳實作政策上，應遵循四個主要安全事項，即安全納入設計、隱私納入設計、資產安全管理、風險與威脅管理。在組織運作上，應建立合適的治理程序，包括對供應商的資安協力要求、對人員的資安意識建立與訓練、安全性管理、資安事件管理。在技術實作上，則應建立技術安全措施，以落實智慧車輛與後端系統的保護，包括偵測資安威脅、對網路與端口之保護、軟體安全、雲端安全、密碼學、存取控制、資安防護與網路服務中斷恢復力、自動駕駛系統自我防護與網路持續運作 [10]。

回歸車聯網支付、管理、通訊三大應用與系統範圍上，分析其可能的威脅風險如下：

1. 支付應用系統：

   聯網汽車通常包括車載資訊娛樂（In-Vehicle Infotainment, IVI）系統，這些系統結合了多媒體，導航，無線電和電話功能，而執行這些功能的軟體需要一個複雜的作業系統來提供底層服務。汽車製造商和一級供應商傾向於採用現有且授權許可的作業系統（如 Linux，Windows 或 QNX）來構建 IVI 系統，就如同建構手機一樣，IVI 系統可以透過整合應用軟體、作業系統和 SoC 來達成，那麼蘋果支付，谷歌支付和三星支付等應用軟體就能夠與 NFC 或藍牙低功耗（BLE）周邊硬體和技術（如 HCE 和 QR 碼）結合使用，即可達到行動支付的目的，例如：駕駛給汽車加油時，可透過 IVI 系統與安全、短距離無線且需授權的加油站泵進行通訊。一旦加完油之後，即可透過網路進行支付的動作 [11]。

   然而行動支付因為皆透過網路進行，所有的數據都曝露在網路上，非常容易受到資安駭客點對點的攻擊，對於應用程式、重要參數及資料都有其風險存在或設備暴露或遭破解，引發系統性風險，資安駭客也會針對使用者認證機制的資料進行竄改或冒用，藉以破壞行動支付體系的安全。

2. 管理應用系統：

   ITS 是一種集中式的管理系統，集中式網際網路面臨很多安全和隱私問題，雖然所有的資料皆存在於數據中心，用於存儲數據並相應

地運行應用程式，但數據儲存中心也有分散風險管理，這並不意味在 ITS 系統功能面不會面臨著惡意攻擊者的威脅，因為所有的功能介面都在控制中心，管理設備也都曝露在外，資安駭客可以藉由外部設備或內部網路的任一結點，進行攻擊，癱瘓設備或網路，讓系統部分或全面性的中斷服務。

3. 通訊應用管理系統：

訊息、數據資料的交換或傳遞是 ITS 生態系統的核心，所有中心和設備都在協調的協定中進行運作，以確保高效能的交通流量和安全運行，這可以是車對車（V2V），車對基礎設施（V2I）和基礎設施對基礎設施（I2I）彼此之間的溝通，資安駭客透過掃描程式找尋漏洞，因為系統上的軟體和硬體或網路上的漏洞很容易被利用，惡意軟體或間諜軟體可以透過漏洞被安裝在系統上散佈不實資訊，擾亂資訊流在 ITS 系統上的正常且正確的運作。

(二)資安標準對照

依據汽車產業之「網路安全管理系統(CSMS)」及「ISO/SAE 21434-道路車輛－網路安全工程」等二項汽車網路安全標準，我們可以發現自車輛整體開發流程(V-model)，包含從設計、製造乃至停產等階段，就已明確規範了相關必要採行的網路安全管理措施，各階段執行的要求必須以「具有安全意識」的需求來進行產品規格分析，確保整個供應鏈都具有支持「安全設計」(security by design)的流程，並且在反覆執行的流程中加入執行結構化的威脅分析和風險評鑑，藉此判斷且決定流程中所需要的保護需求。其中，ISO/SAE 21434 不同於 ISO/IEC 27001 的組織自身安全考量，更著重於整個供應鏈的專案管理，以及強調持續性風險與漏洞管理的監控機制，要求在概念、開發、驗證、生產、營運與維護及退役等階段，必要產出項對應之文件及驗證報告，並透過相應的風險控制方法來實作 [12]。

綜前所述，我們可知針對車聯網的資安要求標準有下列三個目標，其「網路安全管理系統（CSMS）」及「ISO/SAE 21434-道路車輛－網路安全工程」對應章節如表 3：

表 3-車聯網資安要求國際標準對應章節一覽表

車聯網 資安要求目標	國際標準對應章節	
	CSMS	ISO/SAE 21434
協助汽車產業實施網路安全管理方法	第二部分-CSMS 相關需求 第四部份-報告規定	§5 包括組織的網絡安全政策、規則和流程的實施，進行整體網絡安全管理 §6 專案相關的網絡安全管理 §7 定義活動，該活動為正在進行的風險評估和 E/E 系統的漏洞管理提供資訊，直至支援終止 §8 定義了確定網絡安全風險程度的方法
處理車輛及其生產和運營中的潛在網路安全風險	第二部分-CSMS 相關需求	§9 定義項目和相關資產，確定了網絡安全風險，並定義了網絡安全目標 §10 定義網絡安全規範，實現並驗證了特定於項目或組件的網絡安全要求 §11 描述了在車輛等級上某項的網絡安全驗證 §12 規定了與項目或組件的製造，組裝或校準有關的網絡安全方面 §15 包括對供應商管理的要求
建立汽車網路資訊安全與識別	第三部分-車輛類型需求	§13 規定了與網絡安全事件回應，和對項目或組件的更新有關的活動

資料來源：本研究整理

綜合蒐集文獻所論述，我們可知車聯網目前面臨下列三方面的挑戰：

1. 車輛數據安全問題：

例如具有自動駕駛功能的汽車，具有多種形態的感測器裝置，而車輛行駛中獲得的道路高精度測繪數據，與國防等領域息息相關，應得到嚴格監管。

2. 車聯網安全漏洞問題：

目前汽車智慧功能豐富，相應的攻擊面越多，例如汽車數字鑰匙，區別傳統射頻信號的車鑰匙，具有手機 App、NFC 卡多種形式，提供遠程預熱、關閉車窗等控車體驗，但以近三年特斯拉汽車的重大安全漏洞，就有四起與汽車數位鑰匙相關。

3. 新技術應用安全建設不足：

近年來 V2X 做為車聯網新興技術應用廣泛，但 V2X 相應的安全防護能力相對單薄，攻擊者可輕鬆偽造紅綠燈交通信息，控制無人駕駛車輛違背交通信號行駛，影響駕駛安全。

五、防護建議與因應方案

車聯網做為智慧運輸的重要組成部分，可以提高行車安全、減少交通壅塞、提高交通效率和節能減排。然而，與之相關的支付、管理和通訊系統都可能面臨各種資安威脅，需要採取有效措施保障系統安全。以下是針對每個系統類別提出的防護建議及因應方案。

(一)支付系統：

1. 使用加密技術：

使用加密技術可以保護支付交易的機密性和完整性。對於所有支付交易，應該使用加密協議來保護交易中的敏感信息，如用戶姓名、信用卡號、到期日和安全碼等。在加密協議中，可以使用 SSL/TLS 等協議來加密傳輸的數據。

2. 實施多因子認證：

使用多因子認證可以防止未經授權的訪問和使用。建議使用密碼、指紋辨識、臉部識別等多因子認證方式。

3. 構建支付系統防火牆：

使用防火牆可以防止非法入侵和惡意攻擊。建議將支付系統置於一個獨立的網絡中，實現區域網絡隔離和防火牆設置，以防止非法入侵和攻擊。

(二)管理系統：

1. 加強系統管理：

   加強管理，包括強化密碼、實行管理規範、設置日誌記錄、即時監控系統運行狀態等，可有效提高系統的安全性。

2. 建立安全性檢查機制：

   定期進行安全性檢查，發現和解決潛在的安全隱患，減少安全風險。

3. 實現區域網絡隔離：

   將管理系統置於一個獨立的網絡中，實現區域網絡隔離和防火牆設置，以防止非法入侵和攻擊。

(三)通訊系統：

1. 使用加密技術：

   所有車輛之間的通訊應該使用加密通訊來保護數據安全，使用加密技術可以保護通訊交換的機密性和完整性。。

2. 實施身份驗證機制：

   實施身份驗證機制可以防止未經授權的訪問和使用。建議使用數位簽章、公鑰加密等方式進行身份驗證。

3. 監控：

   對車聯網系統進行監控，及時發現異常活動和攻擊，並進行處理。可成立專門的安全運營中心，負責車聯網的安全管理和監控。

六、結論

ITS 的發展確實帶給現今社會極大的便利與創新的契機，但也擴大了資安駭客的攻擊層面，然而 ITS 的資安問題往往因為建置預算不足，或主導者欠缺網路安全的重要性觀念，導致網路安全防護措施不夠完善，當通訊和資料的交換保護能力低時，安全性就會相對薄弱，所以能夠瞭解網路威脅的範圍，並對 ITS 系統從各層面或不同的發展階段，進行分析、評估系統的安全性、便利性和功能性，提早預測或預防各種可能的威脅，依實際需求做出適時地改善，便可確保 ITS 系統處於最佳狀態，「沒有網絡安全，就沒有功能安全！」，預知、預防、解決，永遠都是智慧交通系統最優先，最重要的課題。

車聯網是一個日漸普及的技術，它的出現將帶來許多便利，但同時也帶來了諸多資安風險。為了確保車聯網的資訊安全，我們需要從多個方面

著手，建立全面的資安管理體系，加強供應鏈安全，並定期進行安全檢查。政府部門、民間企業和消費者都應該對車聯網的資安風險有足夠的認識和警覺，共同保障車聯網的安全可靠性。隨著車聯網技術的不斷發展，相信在各方的共同努力下，車聯網的資訊安全問題可以得到有效解決，讓人們能夠更加安心地享受車聯網帶來的各種便利。

參考文獻

1. 智慧交通運輸系統 (ITS)的三重威脅（民107年1月15日）。資安趨勢部落格。民111年4月25日，取自：https://www.cna.com.tw/postwrite/Chi/306721
2. Judith Cheng、Anthea Chuang (民111年5月12日) 車聯網啟動更安全、高效率的智慧交通新時代。EE Times Taiwan。民111年4月25日，取自：https://www.ithome.com.tw/news/147884
3. K. Kelarestaghi, K. Heaslip, M. Khalilikhah, A. Fuentes, and V. Fessmann. "Intelligent transportation system security: hacked message signs." SAE International Journal of Transportation Cybersecurity and Privacy 1, no. 11-01-02-0004 (2018): 75-90.
4. M. Alam, J. Ferreira, and Fonseca, J. (2016). Introduction to intelligent transportation systems. In Intelligent Transportation Systems (pp. 1-17). Springer International Publishing.
5. S. Chakraborty, and S. Ramesh. (2016, January). Technologies for Safe and Intelligent Transportation Systems. In VLSI Design and 2016 15th International Conference on Embedded Systems (VLSID), 2016 29th International Conference on (pp. 56-58). IEEE.
6. R. Blanes, R. A. Paton, and I. Docherty. (2015, January). Public Value of Intelligent Transportation System. In System Sciences (HICSS), 2015 48th Hawaii International Conference on (pp. 1389-1399). IEEE.
7. K. Kelarestaghi, K. Heaslip, M. Khalilikhah, A. Fuentes, and V. Fessmann. "Intelligent transportation system security: hacked message signs." SAE International Journal of Transportation Cybersecurity and Privacy 1, no. 11-01-02-0004 (2018): 75-90.
8. Alam, M., Ferreira, J., & Fonseca, J. (2016). Introduction to intelligent transportation systems. In Intelligent Transportation Systems (pp. 1-17). Springer International Publishing.
9. 王自雄 (民109年9月23日) 無人載具聯網與資安的機遇與挑戰。電腦與通訊。民111年4月25日，取自：https://ictjournal.itri.org.tw/Content/Messagess/contents.aspx?MmmID=654304344321220642 71&MSID=1073040470475723114
10. David Lin（民109年2月11日）。迎接自動駕駛趨勢 — ISO/SAE 21434 將為車輛網絡安全把關。民111年4月25日，取自：

https://medium.com/automotive-cybersecurity/

11. 面對聯網車輛資安挑戰 聯合國推統一規範作準繩（民110年12月17日）。中央社訊息平台。民111年4月25日，取自：https://www.cna.com.tw/postwrite/Chi/306721
12. Kyle (民107年3月13日) 聯網車將驅動聯網或行動支付模式的市場。科技產業資訊室(iKnow)。民111年4月25日，取自：https://iknow.stpi.narl.org.tw/Post/Read.aspx?PostID=14258
13. David Lin（民110年1月13日）。汽車產業「資訊安全管理系統(CSMS)」法規細部解讀。民111年4月25日，取自：https://medium.com/automotive-cybersecurity/
14. 羅正漢 (民110年11月17日) BSI剖析汽車產業資安標準規範，ISO/SAE 21434與TISAX將受重視。iThome。民111年4月25日，取自：https://www.ithome.com.tw/news/147884