VicOne

Driving Automotive Cybersecurity Forward

VicOne 2023年汽車網路威脅情勢報告

內容

前言

隨著汽車產業持續擁抱數位轉型，網路威脅情勢也不斷擴張和演進。汽車的複雜度日益攀升，包括整合了連線能力、自動化和先進駕駛輔助系統(ADAS)，使它們變得容易遭遇網路攻擊與新式威脅。VicOne了解汽車產業在確保車輛安全上所面臨的障礙，知道網路攻擊對車輛運作的嚴重後果，以及該產業面臨的複雜情勢。

這份報告針對當前的網路資安趨勢與影響汽車產業的威脅提供了一份綜合檢視。我們首先回顧了該產業在法規遵循方面的進展，檢視關鍵的網路資安規範以及當IT網路資安套用到汽車領域時的盲點。接著，我們點出車廠最常面臨的漏洞和風險，強調守護資產的重要性。

本報告的另一個重點是案例研究，本文所舉的案例點出了導入最新先進技術時所涉及的風險，強調創新與資安兼顧的必要性。此外，我們也針對最新的網路資安趨勢提出一個獨特的觀點，務實地探討這些演變中的挑戰該如何解決。

我們提出了一些洞察和建議，希望能為汽車製造商(OEM)及供應商指點迷津，協助他們做出明智決策，採取一些策略來保護自己的車輛，使它們免於網路攻擊。這份報告的最終目的，是要提供一些寶貴的資源，協助業界因應今日汽車網路資安複雜性。

重點摘要

法規遵循的挑戰

自從「聯合國第155號規範」(UN R155)在2022年7月正式成為汽車製造商(OEM)必須遵守的一項規範之後，導入各種ISO標準的工作也變得更加急迫。其中一些關鍵的標準包括：ISO 26262、ISO/SAE 21434、「可信任資訊安全評估交換」(Trusted Information Security Assessment Exchange，簡稱TISAX)以及「汽車軟體流程改進和能力測定」(Automotive Software Process Improvement and Capability Determination，簡稱ASPICE)。值得注意的是，ISO 26262與ISO/SAE 21434是OEM需要解決的最大挑戰。

ISO 26262主要針對功能上的安全性，也是OEM廠商通常會優先通過市場認證的領域。反觀ISO/SAE 21434的重點則在於資訊安全，這是許多OEM廠商經常忽略的一個重要面向。ISO/SAE 21434就是針對產業這方面的挑戰，強調嚴密的資訊安全對汽車產業的重要性。

除此之外，根據UN R155的要求，從2024年7月開始，所有新生產的車輛都必須達到這些法規的安全要求，這是業界接下來的一大挑戰。OEM廠商必須開始思考他們能否在這段期限之內完成新流程的導入或現有流程的改善，並且將去年見到的一些重點領域納入考量。

多年來，VicOne一直是走在汽車網路資安的尖端，為各種OEM廠商提供指引並協助其達成所需符合的ISO規範。在接下來的內容當中，我們將深入探討VicOne如何運用自身的豐富經驗，協助我們客戶因應及配合不斷演變的法規情勢。

法規如何要求以及對產業有何影響

面對法規，企業的作法(不論主動或被動)都會受到他們在汽車產業扮演的角色所深深影響。不僅數十年來一直謹守法規的OEM廠商及供應商如此，就連那些才剛開始了解並落實相關標準的廠商也是如此。

ISO/SAE 21434對內部供應鏈管理的要求帶來了一項重大的疑慮，例如，ISO/SAE 21434的RQ-05號要求規定OEM廠商及其供應鏈必須持續通報其產品品質、網路資安治理以及人員組織架構。此處的一大挑戰是：這些要求不僅涵蓋軟體供應商或資訊安全供應商，由於ISO/SAE 21434是建立在ISO 26262所聚焦的功能性安全之上，所以，這些要求將影響整個汽車供應鏈，包括機械零件(如煞車系統或頭燈)供應商在內。

對於已經熟悉ISO流程的下游供應商，要適應這些改變相對單純，他們只需讓現有的認證能符合新的規範，然後完成必要的文件即可。

但對於先前並未拿過這些認證的大多數供應商來說，挑戰卻相當艱難。從實務面看，許多原本就不涉及資訊安全的傳統供應商，很可能缺乏像研發安全(RDSEC)、營運安全(OPSEC)以及產品事件回應團隊(PSIRT)這樣的特殊部門。同時，對OEM廠商來說，要大幅重整其供應鏈並不切實際，尤其是那些以穩定為優先的關鍵元件。供應商無法跟上必要的ISO認證，已迫使許多OEM廠商開始探索其他替代解決方案。

滲透測試與漏洞管理作為遵循ISO/SAE 21434規範的替代方案

儘管ISO/SAE 21434標準要求OEM廠商必須對其設計進行徹底的安全驗證，然達成這項標準的作法卻沒有硬性規定。對於目前已經有嚴格的品質管理、開發管理及完整網路資安團隊的企業來說，他們可以調整現有的流程來達到法規要求，但其他沒有這類系統的企業，還是有其他方法可以遵守ISO/SAE 21434的要求。該法規的主要理念是，廠商要能證明他們的產品在「設計上即具備安全」(secure by design)，所以，任何方法只要能證明其設計是安全的就可以，例如，通過團體討論或聘請第三方機構進行滲透測試或漏洞管理。這與業界內的其他ISO標準截然不同，例如：ISO 26262所訂定的危害分析與風險評估(HARA)流程就必須嚴格遵守。

回到滲透測試與漏洞管理的議題，IT產業採用這些方法已有數十年之久，例如，ISO/IEC 27001就是管理資訊安全的一套國際標準。目前在大型企業之間已逐漸接受滲透測試與風險評估應該是一件常態性的工作。然而很重要的一點是，傳統專為提升IT資產設備安全而設計的滲透測試，與ISO/SAE 21434所著重的要點有很大差異，因為後者的目標是要提升整體的道路安全。

滲透測試的極限

ISO/SAE 21434的終極目標是提升道路安全，任何利用滲透測試來達成ISO標準的評估方法首先必須考慮一個問題：萬一目標(受測對象)發生故障，會不會影響道路安全？這個觀點通常與許多網路資安廠商的優先考量不同，因為傳統上他們都依賴像「通用漏洞評分系統」(Common Vulnerability Scoring System，簡稱CVSS)這類專為評估IT系統威脅而設計的評分系統。但對於車輛系統來說，最重要的永遠是道路安全。滲透測試的問題是，其評估指標是專為IT產業而設計，滲透測試報告經常包含了許多微不足道的發現，這對於改善車輛的道路安全或遵守ISO標準並沒有太大幫助。

所以，OEM廠商會發現自己花了大把鈔票，但得到的卻是一大堆不相干的資訊。因此，找到一家同時具備汽車硬體與電子系統專業能力的車用資安廠商就變得至關重要。

漏洞管理的角色以及建置不當的後果

除了滲透測試之外，漏洞管理的市場需求也在迅速成長，此現象的主要帶動因素是UN R155和ISO/SAE 21434。UN R155將其網路資安管理系統(CSMS)的要求濃縮在一條很大的規定之下，也就是企業必須管理車輛整體生命週期的網路資安。而ISO/SAE 21434也規定，具備網路資安特性的元件在其整體生命週期當中都要有漏洞管理。這使得以軟體物料清單(SBOM)為基礎的漏洞管理服務大量出現。某些急於切入這市場的傳統IT資安廠商匆促地推出了一些相關服務，對OEM廠商帶來了挑戰。某些SBOM掃描產品為了爭取市場能見度，宣稱可偵測上千個(甚至上百萬個)漏洞。但從客戶的反應顯示，這些偵測到的漏洞大部分都是誤判，而且很少跟道路安全有關。

解決TARA流程中的挑戰

ISO/SAE 21434另一個很重要的部分就是「威脅分析與風險評估」(TARA)流程。VicOne觀察到TARA顧問服務在2023年爆紅，TARA勢必成為OEM廠商與供應商的另一個重大障礙。

乍看之下，確保車輛與元件受到保護以防範網路威脅似乎並不困難，看起來跟滲透測試與漏洞掃描想要達成的差不多。但是若仔細檢視ISO/SAE 21434的文件就會發現一項更廣泛且關鍵的要求，它明文規定：[1]

> 發掘威脅情境的方法可透過團體討論和/或系統性方法，例如：
>
> - 從合理可見的誤用和/或濫用當中推導出惡意使用的情境。
> - 根據框架(如EVITA、TVRA、PASTA、STRIDE)來建立威脅模型(假冒、篡改、拒絕、資訊外洩、阻斷服務、提升權限)的方法。

這麼廣大、無限制的範圍卻沒有具體的指引，ISO/SAE 21434的基本目標是要解決可能破壞車輛安全的潛在網路資安問題，儘管這對壽命動輒超過10年的汽車來說是一項完全合理的要求，但要實行起來很可能極其麻煩。撇開人力的考量不談，光是要決定這項要求該從何下手，就讓人頭皮發麻。

儘管市場上已經有不少產品和服務宣稱可以幫忙建立前述流程，但大多數的解決方案只不過是一些可幫忙整理報表或摘要節錄ISO/SAE 21434條文的工具，吃重的工作大部分還是得靠OEM廠商和供應商自己。ISO文件列舉了兩種主要方法：團體討論與系統性分析。所謂的「團體討論」非常直覺易懂，也就是找來網路資安與車輛安全的專家。但「系統性」方法，就不是那麼明確，當考慮到每一個可能的情境時，企業是否也必須親自下海參加腦力激盪，一起發揮想像力？

ISO顧問通常會建議從以資產為核心的方法著手，針對每一個元件發掘其可能故障的情境。一方面，汽車供應鏈上的研發人員確實可以仔細思考其程式碼可能失敗的情境，另一方面，對於網路資安人員來說，他們可以用過去發生的資安事件案例作基礎，預測元件失敗或故障的可能情況。理想情況是，只要整合來自研發和資安部門兩邊的見解，應該就能完整掌握威脅的情境，做好威脅可行性與潛在攻擊路徑的評估。然而，想要預測還沒發生的事件，例如網路攻擊，對研發部門來說有點虛無飄渺。再者，這是兩種截然不同的專業能力，而且IT資安所發生的前例，不一定能順利轉化成汽車安全的標準。這兩項因素加起來，會讓這種試圖窮盡潛在可能性的方法變成一項重大挑戰。除此之外，ISO/SAE 21434在TARA一節也是充滿模糊空間與不明確的要求，使得大多數企業若不投入大量的財力和人力來進行必要的討論，很難將其流程標準化。

那麼，OEM廠商與供應商該如何解決TARA流程的挑戰？VicOne從其獨特的觀點想出了一套方法可以讓OEM廠商的TARA建置團隊建立高效率的標準作業程序(SOP)。這套方法是以我們汽車威脅情報為基礎，忠實反映了真實世界的威脅，省去多餘的步驟。所以，這套策略能大幅簡化OEM廠商的TARA流程，讓他們更平順地轉換至ISO規範。

威脅情勢回顧

前一節，我們探討了法規的情勢，了解了法規遵循上的相關挑戰，以及如何避開一些錯誤的方法。這一節，我們將透過我們累積的網路資安漏洞與事件案例來釐清目前產業所面臨的問題，協助廠商解決其系統或車輛可能存在的相關問題。

數百個已通報漏洞

我們一直努力監控與汽車元件和服務相關的「通用漏洞及弱點」(Common Vulnerabilities and Exposures，簡稱 CVE)。根據我們從2019年以來的觀察，已通報的CVE數量非常多(每年超過200個，而且光2023上半年就超過這個數量)，顯示近年來汽車網路資安已獲得更大的關注。

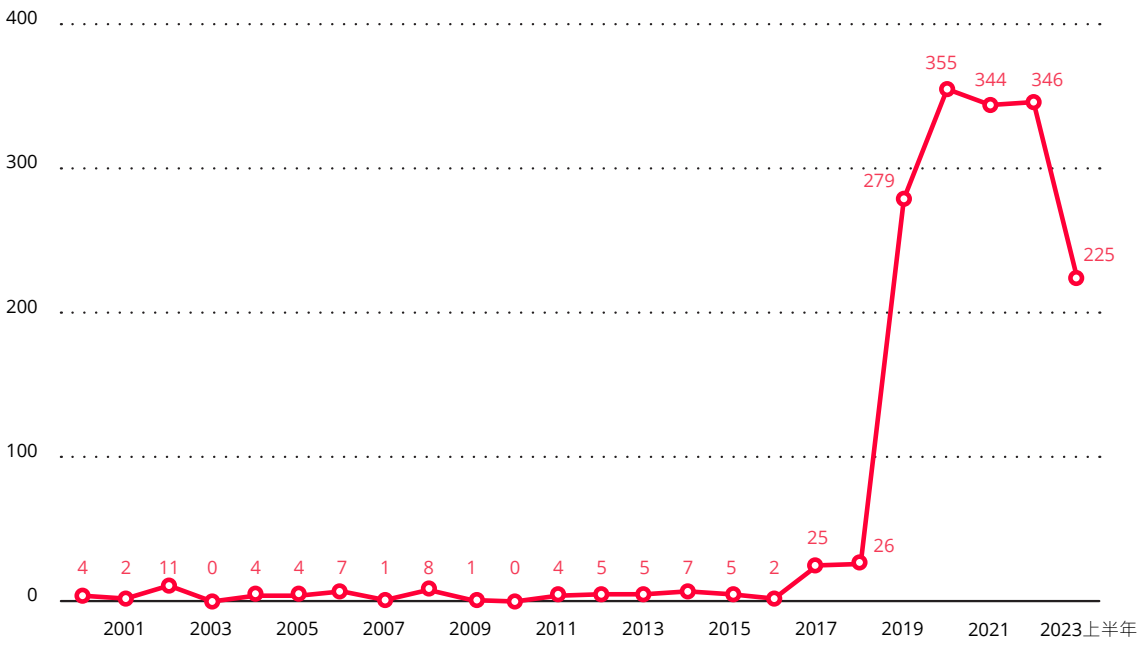

圖 1：從2000年至2023上半年的CVE數量。

下表摘要顯示我們在CVE當中發現的「通用弱點列表」(Common Weakness Enumeration，簡稱 CWE)漏洞。很清楚地，其中最常見的問題是：越界寫入(OOBW)、越界讀取(OOBR)、緩衝區溢位、使用已釋放記憶體，以及輸入檢查不確實。從我們2023上半年蒐集到的資料可看到各種網站或應用程式管理的SQL隱碼注入案例。大多數有關整數溢位(integer overflow)或越界繞回(wraparound)漏洞的問題都發生在各種晶片組的元件當中。

CWE ID	名稱	說明
CWE-787[2]	越界寫入	產品寫入資料的位置超過原本預定的緩衝區末端之後或開頭之前。
CWE-416[3]	使用已釋放記憶體	參照已經釋放的記憶體，有可能導致程式當掉、使用非預期的數值，或執行不應當執行的程式碼。
CWE-125[4]	越界讀取	產品讀取資料的位置超過原本預定的緩衝區末端之後或開頭之前。
CWE-120[5]	複製緩衝區時未檢查輸入大小 (典型的緩衝區溢位)	產品複製輸入緩衝區的內容到一個輸出緩衝區，卻未檢查輸入緩衝區的大小不能大於輸出緩衝區，進而導致緩衝區溢位。
CWE-20[6]	未確實檢查輸入資料	產品收到輸入或資料，但卻未加以檢查或檢查不實，導致輸入資料無法安全或正確地處理。

表 1：所有已發布的CVE當中與汽車產業相關的前5大CWE。

CWE ID	名稱	說明
CWE-125	越界讀取	產品讀取資料的位置超過原本預定的緩衝區末端之後或開頭之前。
CWE-787	越界寫入	產品寫入資料的位置超過原本預定的緩衝區末端之後或開頭之前。
CWE-120	複製緩衝區時未檢查輸入大小 (典型的緩衝區溢位)	產品複製輸入緩衝區的內容到一個輸出緩衝區，卻未檢查輸入緩衝區的大小不能大於輸出緩衝區，進而導致緩衝區溢位。
CWE-89[7]	未確實將SQL指令中用到的特殊元素歸零(SQL隱碼注入)	產品在組合一個SQL指令時用到來自上游元件受外部影響的輸入資料，但卻沒有將某些可能改變SQL指令預期效果的特殊元素歸零和或正確歸零就傳遞給下游的元件。
CWE-190[8]	整數溢位或越界繞回	產品執行了某項運算可能發生整數溢位或繞回的情況，但程式的邏輯卻假設運算結果永遠大於原本的值。當運算結果會用於資源的管理或決定程式碼的執行時，可能會衍生其他的弱點。

表 2：2023上半年所有已發布的CVE當中與汽車產業相關的前5大CWE。

晶片組或系統單晶片(SoC)上發現的問題占了2023上半年已通報CVE的多數，其次是第三方管理應用程式以及車載資訊娛樂(IVI)系統的漏洞。

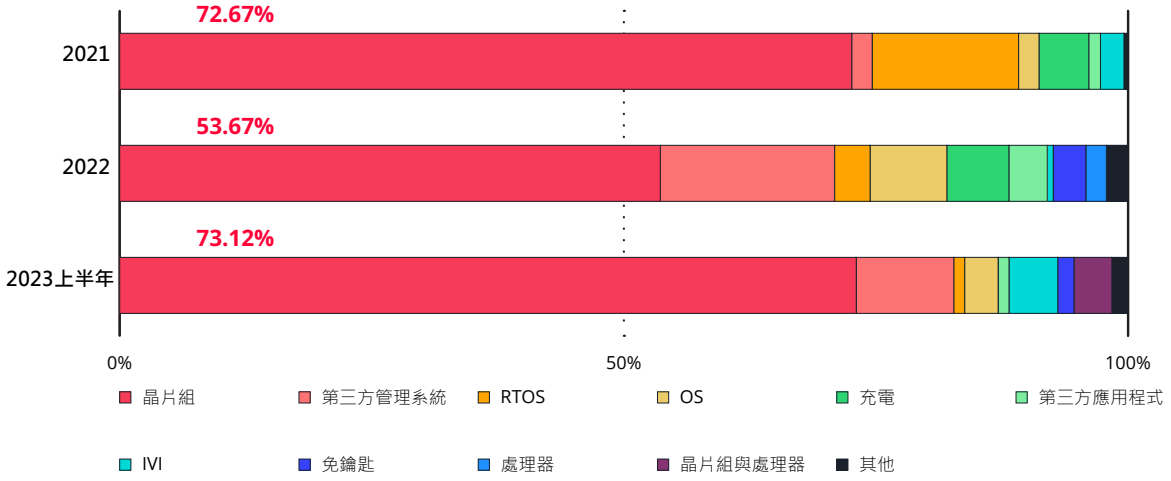

圖 2：前幾大CVE漏洞涉及的對象(CVE2021、2022及2023上半年)。

網路攻擊與資安事件的增加

除了汽車或其系統本身的漏洞之外，我們也蒐集了為數不少的汽車資安事件案例，並加以分類。這些案例大部分都是網路攻擊、防盜鎖出狀況，以及應用程式和應用程式開發介面(API)相關的問題。

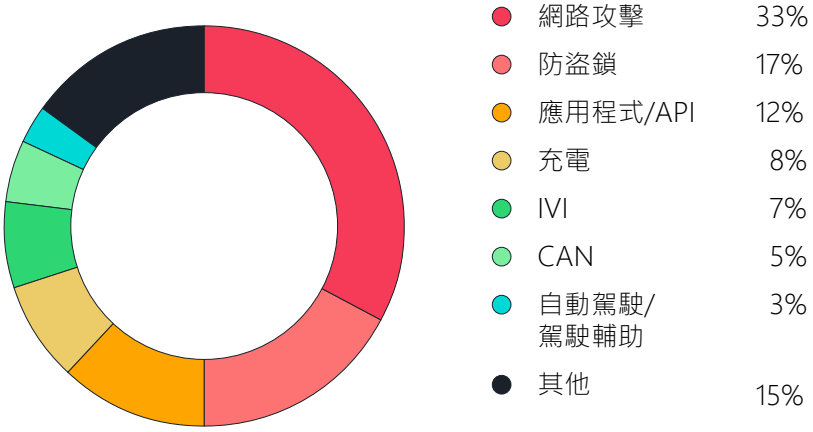

圖 3：資安事件類別分布情況(2022下半年至2023上半年)。

進一步檢視網路攻擊事件就可以看清楚，這些案例有不少都是起源於第三方服務與診斷供應商，以及汽車元件供應商，包括：製造商、物流廠商、服務供應商，以及負責生產元件、配件或零件的企業。

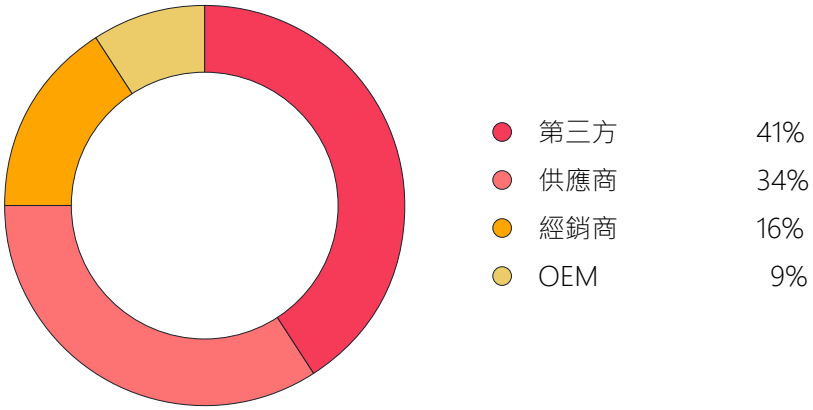

圖 4：網路攻擊案例類別分布情況(2022下半年至2023上半年)。

此外，我們也估算了2021至2023年網路攻擊事件的財務衝擊，導致這些後果與成本的因素包括：勒索病毒攻擊、資料或個人身分識別資訊(PII)外洩，以及系統停機期間的相關損失。這些費用僅計算技術和營運相關的有形成本，不包含品牌、公關、銷售及行銷費用等無形成本。

費用(美金)	2021	2022	2023上半年
勒索病毒損害	74,755,025美元	142,003,000美元	209,675,448美元
資料外洩/PII曝光	13,795,000美元	4,000,000美元	9,574,700,000美元
系統停機成本	1,300,385,123美元	802,432,329美元	1,998,351,233美元
損害成本總計	**1,388,935,148美元**	**948,435,329美元**	**11,782,726,681美元**

表 3：網路攻擊損害成本估計(2021年至2023上半年)。

這些估計意味著有更多網路攻擊似乎正在瞄準與影響汽車產業，而且這樣的成本將繼續攀升。

區域性資料

2023上半年大多數的網路攻擊都是由北美與歐洲所通報，延續了2022年所看到的趨勢。不過在一般資安事件方面，亞太地區2023上半年的通報數量顯然占了不少。

北美	43%
歐洲	30%
亞太地區	20%
全球	6%
非洲	1%

表 4：汽車產業已通報資安事件的區域分布情況(2022年)。

北美	31%
全球	28%
亞太地區	23%
歐洲	13%
南美/拉丁美洲	5%

表 5：汽車產業已通報資安事件的區域分布情況(2023上半年)。

北美	45%
歐洲	32%
亞太地區	21%
南美/拉丁美洲	1%
全球	1%

表 6：汽車產業已通報資安事件中的網路攻擊事件區域分布情況(2022年)。

歐洲	41%
北美	41%
亞太地區	13%
南美/拉丁美洲	3%
非洲	1%
阿拉伯國家	1%

表 7：汽車產業已通報資安事件中的網路攻擊事件區域分布情況(2023上半年)。

區域	國家/地區	
亞太地區	澳洲	菲律賓
	中國	新加坡
	印尼	南韓
	日本	台灣
	馬來西亞	
歐洲	法國	西班牙
	德國	瑞士
	義大利	土耳其
	荷蘭	英國
北美	加拿大	美國
南美	墨西哥	

表 8：已通報汽車網路攻擊的國家/地區(2022年)。

區域	國家/地區	
非洲	模里西斯	
阿拉伯國家	摩洛哥	
亞太地區	澳洲	南韓
	印度	台灣
	日本	泰國
	新加坡	
歐洲	比利時	波蘭
	捷克	葡萄牙
	丹麥	俄羅斯
	法國	西班牙
	德國	瑞典
	希臘	瑞士
	義大利	土耳其
	荷蘭	英國
	挪威	
北美	加拿大	美國
南美	巴西	祕魯
	墨西哥	

表 9：已通報汽車網路攻擊的國家/地區(2023上半年)。

案例研究

了解了當前的威脅情勢之後，現在讓我們來深入研究三個案例以點出我們最重要的幾項觀察，包括CPU、CAN注入以及應用程式/API相關的重大漏洞。

從這幾個案例就能看出汽車生態系眼前的漏洞以及新導入的技術如何擴大車輛可攻擊面並帶來新的風險。此外，也點出駭客可經由哪些途徑來竊取或洩露敏感的資料，除了取得車輛的控制權之外。

Zenbleed

2023年7月，一名Google資安研究人員Tavis Ormandy披露了AMD Zen 2 CPU微架構的一個令人擔憂的重大漏洞[9]，此漏洞造成了一項嚴重威脅，可能導致敏感的資料以每核心30 kbps的速度急速外洩。

過去，CPU與車輛在功能上並無直接的關聯，但軟體定義汽車(SDV)的出現改變了這個情況。現在，越來越多的汽車都配備了強大的CPU來提升功能。由於駕駛輔助與自動駕駛之類的先進功能逐漸普遍，汽車更加仰賴強大的CPU和GPU來處理這些功能所需的複雜運算。

為了回應業界的需求，AMD推出了自家的汽車數位座艙解決方案，有可能獲得汽車製造商的青睞。不過，採用AMD Zen CPU為核心處理器的車輛可能會受Zenbleed漏洞影響，這是一個嚴重的資安風險。此漏洞可能會造成機敏資訊外洩，包括：密碼與金鑰(token)，進而損害車輛與乘客的安全和隱私權。

防範之道

對於受到影響的系統來說，解決Zenbleed漏洞是當務之急。由於CPU硬體無法透過修改CPU電路的方式來修補，因此需要替代的解決方法。此漏洞已通報給AMD，而該公司也已釋出了韌體微碼(microcode)更新來解決這項問題。採用這批AMD CPU的OEM廠商可透過無線(OTA)更新的方式來套用微碼更新，或者將產品召回，視車輛的更新機制如何。對於無法套用微碼更新的情況，還是有軟體替代方法可用。只要將晶片內建的「chicken bit」開關切換成DE_CFG[9]，就能防範這個漏洞。不過，這個替代方法也有它的代價：套用軟體修正可能會影響效能，因為漏洞的源頭就位於效能最佳化技巧當中。

從威脅情勢的發展來看，硬體漏洞是不太容易發生、同時也不常見的問題。不過，當這類問題出現時，卻會造成嚴重影響。畢竟，硬體漏洞本來就很難修正，而CPU漏洞又是最難修正的一種。廠商幾乎不可能透過更換CPU來解決問題，儘管某些缺陷可以透過微碼更新的方式來修正，但軟體式修正有時會導致CPU跑起來變慢，解決了一個問題卻引來另一個問題。要防範CPU漏洞得看問題而定，但很不幸地，許多問題基本上是無解。但基於法規要求，還是有必要加以防範。廠商必須找出可能造成損害的情境，並且在損害真正發生之前預先解決。由於硬體漏洞(尤其是CPU漏洞)幾乎無法徹底解決，所以必須借助一些其他機制，包括OTA更新，以及關閉除錯介面之類的硬體保護，並且做好實體安全。

CAN匯流排注入

「控制器區域網路」(Controller Area Network，簡稱CAN)匯流排是1980年代制定的一種通訊協定，專為汽車的各種應用所設計。在CAN匯流排推出之前，汽車製造商得靠多個點對點連線來做到同樣的事，導致車內的線路複雜而紊亂。今日，CAN匯流排已是汽車產業廣泛採用的一項標準，幾乎所有現代化車款都採用。CAN匯流排也許不是什麼鮮光亮麗的技術，但對汽車產業來說卻是個成熟嚴謹的系統。儘管它存在著一些已知問題，例如：匯流排關閉攻擊(bus-off attack)[10]、CANCAN攻擊[11]以及WeepingCAN攻擊[12]，但仍是目前最棒的車用通訊技術。

CAN匯流排的一項最新資安挑戰就是CAN匯流排注入攻擊，這是由Ian Tabor和Ken Tindell所發現[13]。這項攻擊技巧可讓歹徒更容易地將車偷走，而今年也經常看到嫌犯利用這種手法。許多人都不知道，這是2023上半年通報次數最多的威脅，畢竟它跟CAN匯流排及防盜器的威脅息息相關，所以這問題對汽車的設計有很大影響。以下是此手法可能的攻擊情境：

- 駭客經由車輛的頭燈循線找到CAN匯流排線路，此線路會連到智慧鑰匙的接收器電子控制單元(ECU)。

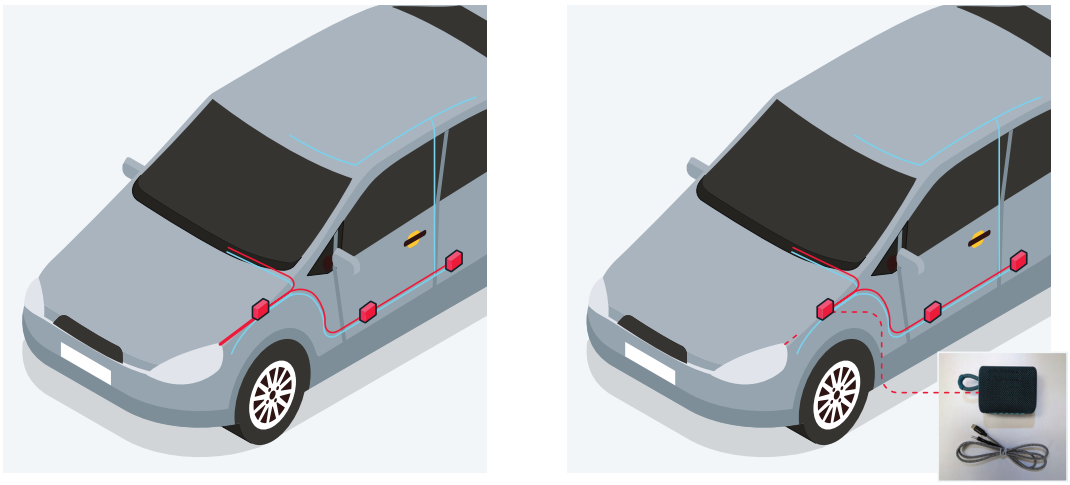

圖 5：左：頭燈還連著車輛的CAN匯流排。右：已經被換成了CAN注入器。

- 當CAN注入器電源開啟後，駭客就能發送一個喚醒的訊框來不斷喚醒CAN匯流排，直到該裝置收到回應為止。
- 收到回應之後，CAN注入器就會利用仲裁機制試圖強制接管電路。此電路會防止其他裝置在CAN匯流排上傳送訊號，並關閉CAN匯流排通訊協定的錯誤處理機制，避免其他ECU阻礙CAN注入器的介入，同時越過硬體安全機制。
- 接著，CAN注入器就能假扮成智慧鑰匙的ECU，然後密集發送假訊息給車輛的閘道ECU，例如「鑰匙已通過驗證，請解除防盜器」。
- 閘道ECU接著將假訊息複製到另一個CAN匯流排。

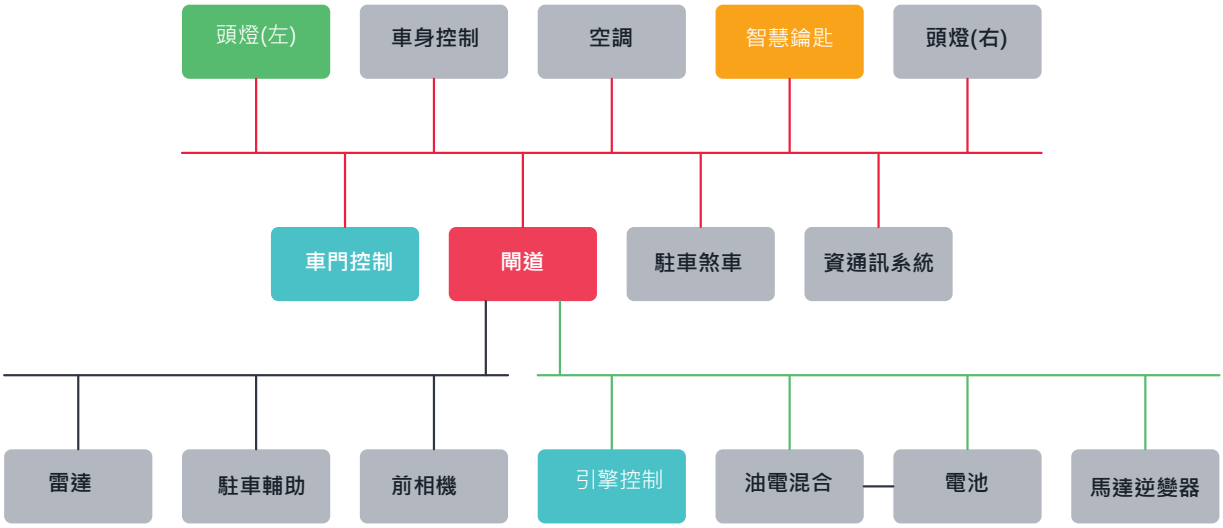

圖 6：簡化的失竊車輛CAN匯流排示意圖(根據Ken Tindell提供的原圖[14])。

- 引擎控制系統接收道這個假訊息，然後關閉了防盜功能。
- CAN注入器接著密集發送另一個假的CAN訊息給控制車門的ECU來解鎖車門，例如「鑰匙有效，請解鎖車門」。

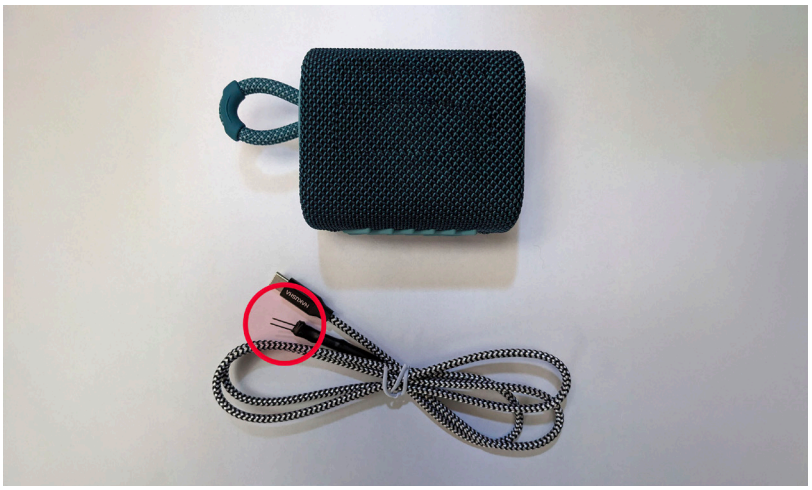

圖 7：解鎖工具組。紅圈標示處對應匯流排的兩個針腳：CAN High和CAN Low，用來連上車輛的CAN匯流排(根據Ken Tindell提供的原圖[15])。

根據網路上最早的庫存網頁顯示，這套工具是從2022年6月18日開始在Keyless Go Repeater網站上販售[16]，我們查了一下庫存網頁，其售價是每組3,500歐元(約3,700美元)。雖然我們無法確定這就是它最早的上市價格，但我們知道它從2022年便已經在販售。此外我們也快速搜尋了一下，發現這套工具在各種網站上的價格通常介於1,500歐元(約1,600美元)至5,000歐元(約5,300美元)之間。這套工具的外觀通常像一個小盒子，但有些版本會設計得很像JBL藍牙喇叭或Nokia 3310手機。由於有這樣的偽裝，執法人員有時就算發現了也不知道它真正的用途。

廠商	價格
Keyless Go Repeater[17]	4,500歐元(約4,700美元)
Shop-Auto-PODOLSK[18]	4,000美元
AutoDecoders[19]	1,500歐元(約1,600美元)
Agent Grabber[20]	4,500歐元(約4,800美元)
UnlockCars Grabber[21]	3,500歐元(約3,700美元)
Kodgrabber[22]	5,000美元

表 10：解鎖工具組在各種網站上的價格(2023年8月)。

防範之道

依據Tindell的建議，有兩種方法可以阻止駭客：暫時性及永久性。

暫時性的解法是：只要對閘道ECU重新程式化，讓它唯有在一定時間內未偵測到錯誤時才轉發訊息，就能可防止注入器在CAN匯流排上製造錯誤然後發送智慧鑰匙的CAN訊框。這是根據CAN注入器的功能來過濾訊息。不過，駭客可能很快就會調整作法並想出類似的攻擊。

永久性的解決方法是採用零信任的作法，讓CAN裝置在預設狀況下不信任來自其他ECU的訊息。然後在CAN訊框當中加入額外的驗證機制來確認ECU的真實性(沒有被偷換掉)。要做到這點，就必須配發私密金鑰給ECU，並且與車輛配對。

這套防範策略是從技術的角度出發，但若從法規的角度來思考，還有其他的防治方法可用。例如，啟用閘道ECU的OTA更新來提供即時的適應能力，而且，監測訊息的改進也有助於早期偵測威脅。除此之外，也可透過實體安全的強化來增加一層額外防禦。這些額外的措施，都應該納入損害情境的考量當中，以建立一道更堅固的壁壘來防範潛在的駭客。

汽車雲端服務入侵

連網汽車最關鍵的一項功能就是能連上網際網路，可同時存取網路資源並傳送監測資料。這項能力徹底改變了汽車，使它從一台交通工具轉型為一個可提供珍貴資訊及執行某些功能的裝置。下圖是我們對連網汽車生態系的願景：現代化連網汽車就如同一台裝了輪子的智慧型手機，而第三方應用程式則扮演了提供駕駛人與乘客體驗的重要關鍵。

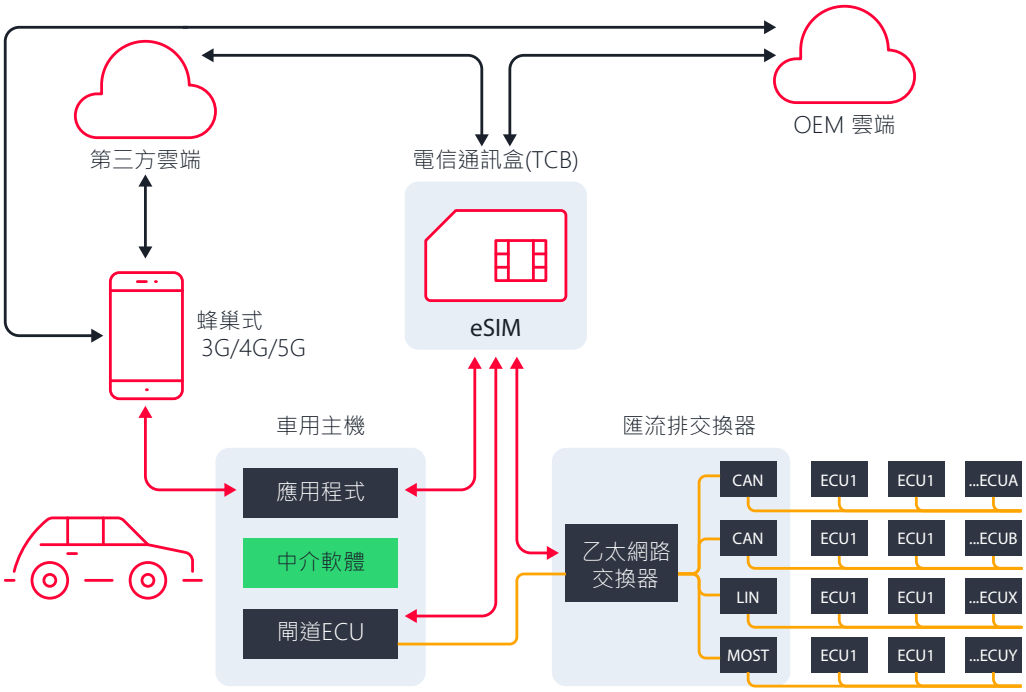

圖 8：雲端連網的汽車架構[23]。

大多數的連網汽車都會連上OEM廠商或第三方的雲端來存取各種服務和資料。儘管這樣的設計架構似乎合理且必要，但卻引來了新的挑戰。

在一篇2023年1月發表的部落格中，網站應用程式資安研究員Sam Curry與其團隊展示了如何利用車載資通訊系統(telematic system)與API的漏洞來進入各家OEM廠商的後台雲端基礎架構。以Mercedes-Benz為例，他們發現了一個專為車輛維修廠打造的公開網站，該網站能寫入資料到核心員工的LDAP (Lightweight Directory Access Protocol)系統所使用的資料庫。他們先在這個網站註冊以取得有限的權限來使用員工可使用的應用程式，然後再利用這些應用程式進一步存取敏感的內部應用程式，包括 Mercedes-Benz GitHub，並在這裡找到如何建立應用程式來與客戶車輛通訊的詳細說明[24]。

此一發現傳達了一個明確的訊息：汽車產業無法倖免於IT產業雲端服務所面臨的相同問題。但相形之下，汽車產業卻沒有充分的準備來妥善處理這些問題。

弱點分析

根據Curry和其團隊的發現，我們整理了一份受影響的雲端服務網站可能存在的CWE漏洞清單。這裡點出了一個簡單的事實，那就是：這些問題已經在IT產業發生過數千次，但汽車產業可能直到現在才知道它們的存在。

此處點出的雲端相關問題分可為兩種。第一種跟認證和授權有關，第二種則跟輸入參數是否經過確實淨化有關。在認證方面，API可能缺乏適當的存取控管，進而衍生預先認證的問題，導致個人識別資訊(PII)遭到存取。在授權方面，API可能未充分檢查使用者的權限或者可能直接就信任了使用者的請求。至於第二個問題，也就是輸入參數必須經過確實淨化，解決之道就是一條簡單的原則：絕不相信任何使用者，也就是「輸入資料的檢查與淨化永遠都很重要」。輸入資料檢查是一種撰寫程式的技巧，目的是要確保唯有格式正確的資料才能進入軟體系統的元件[25]。這概念也許已經是眾所周知的程式設計原則，但對於缺乏正確程式設計指引或持續整合/持續部署(CI/CD)的環境來說，依然是一項挑戰。

CWE ID	名稱	說明
CWE-20	未確實檢查輸入資料	這項弱點的發生是因為軟體未檢查或未確實檢查輸入的資料，可能導致程式的執行或資料流程發生改變。
CWE-287	未確實做好認證	這項弱點的發生是因為系統未確實認證使用者的身分，可能讓駭客有機會冒充合法使用者。
CWE-284	未確實做好存取控管	這項弱點的發生是因為軟體未檢查使用者或執行程序是否有必要的權限來執行某項動作，可能導致未經授權的存取或資料遭篡改。
CWE-639	不安全的直接物件參照(IDOR)	這項弱點的發生是因為應用程式將內部程式實作的物件(如資料庫記錄)暴露在外，導致駭客無須經過授權就能使用這些物件，進而存取資料。
CWE-89	SQL隱碼注入	這是一種程式碼注入技巧，在輸入欄位暗中插入惡意的SQL指令讓資料庫執行，導致資料損毀或遭到刪除。這類問題通常是因為使用者輸入資料未確實過濾，或者未正確處理一些特殊的字元。
CWE-798	使用寫死的登入憑證	此問題指的是大剌剌地將登入憑證(如：使用者名稱或密碼)寫死在原始程式碼內，被駭客用來非法進入系統。

表 11：根據Sam Curry及其團隊的發現結果所整理出來的CWE漏洞清單。

防範之道

最理想的情況是，這些問題在設計階段就被發現，或是聘請滲透測試人員在早期測試階段發現，不讓問題延續到生產階段。然而，汽車產業的開發流程傳統上都比較關注車輛本身的安全性，而非資安，所以現在才有法規要求他們多一些注意力在網路資安層面。所幸，IT領域已經有一些成熟的作法可以解決汽車產業的問題。下表整理出一些IT界常用、但同樣也樣適用於汽車產業的方法。

方法	方法說明	行動	行動說明
教育訓練	定期舉辦有關程式碼設計安全的訓練，能幫助開發人員避免一些常見的程式設計陷阱。	實務工作坊	舉辦實務工作坊來讓開發人員透過實作的方式親身體驗如何解決資安問題。
		程式設計安全	遵守程式設計安全標準來防範常見的漏洞。
軟體開發生命週期(SDLC)	在軟體開發生命週期的每一個階段融入資安，而不是最後才做，這樣有助於及早發掘及防範漏洞。	設計上即具備安全	從一開始的設計就考慮到安全性。
		程式碼審查	同儕之間彼此互相審查程式碼，有助於避免潛在的問題演變成漏洞。
		靜態應用程式安全測試(SAST)與動態應用程式安全測試(DAST)	這些都能自動偵測程式碼中某些類型的漏洞。
外部稽核	定期交由外部專家進行資安稽核，有助於發掘漏洞，並提供一份獨立的應用程式安全評估。	滲透測試	模擬攻擊系統的流程，來發掘潛在的漏洞。
		漏洞懸賞	透過獎勵計畫來鼓勵通報軟體漏洞，尤其是安全方面的漏洞。

表 12：一些IT界常用、但同樣也適用於汽車產業的最佳實務方法。

改善資安的一項關鍵因素就是企業高層的支持，因為強化安全有可能衍生一些新的問題，導致專案時程延後，它需要強大的人力與財力支援，但成果可能不會立竿見影。不過，從長期的角度來看，這些工作的成效通常是無價的。因為，就法規的角度而言，這些工作不僅是一種有效的防範策略，更可主動降低風險的發生機率。

產業趨勢

幾年過去了，汽車產業現在已經更清楚了解自身的需求，目前絕大多數的發展趨勢都是由標準與法規所驅動，因為所有的車廠都必須遵守法規。廠商的注目焦點已經不再是最強的功能，現在每家廠商都必須證明自己確實有遵守法規，才能獲得車輛的銷售許可，讓車輛進入市場。這一節，我們將逐一探討當前的幾項趨勢。

法規遵循

正如前面提到，法規遵循對今日的汽車產業至關重要，法規遵循涵蓋了眾多要求，因此像TARA與滲透測試這樣的工具，對於達成要求很有幫助。

TARA

2021年3月，「聯合國歐洲經濟委員會」(United Nations Economic Commission for Europe，簡稱UNECE)發布了UN R155規範[26]，隨後在2021年8月，ISO/SAE 21434標準發布，聚焦在車輛電氣與電子(E/E)系統的網路資安。這兩份文件都強調TARA工作在車輛生命週期中的重要性。

TARA的四項主要目標是：威脅發掘、風險評估、風險優先次序判斷，以及防範建議。正如前面指出，OEM廠商通常不擅長威脅情境與攻擊路徑的分析。了解TARA的各個面向，有助於解決相關的挑戰。其整體流程好比在混亂的叢林當中尋找寶藏一樣：掌握地圖是找到目標的關鍵。TARA則可幫忙在地圖上找出最佳路徑。

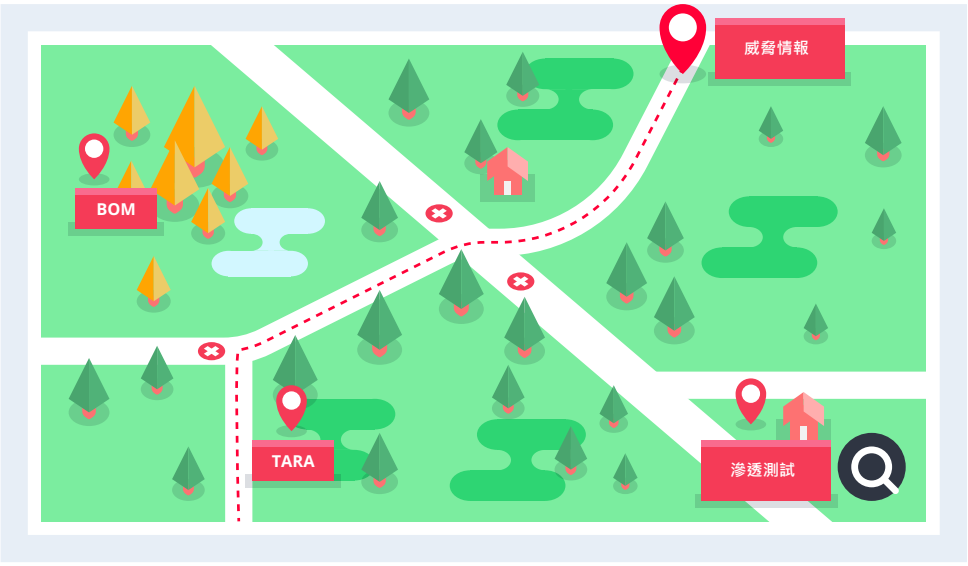

圖 9：運用TARA及其他必要工具來找出潛在問題。

企業若要符合法規，就需要各種必要的工具，我們拿前一張圖來對應做說明：

- 完整的物料清單(BOM)，包括軟體物料清單(SBOM)與硬體物料清單(HBOM)，可提供地形地貌的詳細資訊。
- 品質威脅情報，可幫忙定位寶藏的確切地點。
- TARA可幫忙規劃到達目標的最佳路徑。
- 滲透測試可幫忙放大檢視，將目標在地圖上的位置看得更清楚。

每樣工具都很關鍵。少了一樣，就會讓改善資安、解決最迫切資安問題的目標更難達成。

整個過程當中，TARA扮演著中樞的角色，它就像是一張行動藍圖。不過，它還得仰賴其他工具和資訊的配合。錯誤的威脅情報會讓人走錯路而浪費時間，這突顯出情報品質的重要性。同樣地，滲透測試對於找出「寶藏」(也就漏洞)的確切地點非常重要。

TARA並非一次性工作，但它提供了一個車輛該如何設計的藍圖，以及如何預防潛在傷害的策略。

滲透測試

根據我們的觀察，汽車產業的滲透測試請求，幾乎100%都是為了驗證是否能符合ISO/SAE 21434的網路資安目標。通過滲透測試雖然無法百分之百保證就能符合法規，但確實能協助OEM廠商檢視其產品或系統在一些非預期狀況下的表現。

滲透測試的悠久歷史最遠可追溯至1972年James P. Anderson所做的第一次滲透測試，他提出的漏洞發掘步驟也成了今日滲透測試流程的基礎[27]。在今日來看，滲透測試就是要模擬外部駭客的攻擊，進而評估潛在的網路威脅。在IT領域，滲透測試的方法與流程多年來已經相當成熟。值得一提的是，滲透測試經常被人與品質確保(QA)搞混，但兩者是截然不同的東西。QA測試的重點在於流程，但滲透測試的重點在於披露程式結構中的錯誤。

那麼，汽車產業的滲透測試與IT產業有何不同？在IT產業，滲透測試大多用來發現被忽略的漏洞，以便加以修補。當眾多API的其中之一被發現存在著某種漏洞時，所有相關的API都必須全部重新檢討。這是因為它們通常是由同一個開發團隊所撰寫，因此同樣的問題有可能重複出現在好幾個地方。所以最好做一番全面的檢查，以減少將來可能發生的損害。有時候，這些問題或許不是程式碼的漏洞，而是邏輯或架構上的漏洞。而這類問題幾乎無法在QA流程當中發現，這就是滲透測試能幫得上忙的地方。

不過汽車產業的滲透測試要比IT產業的滲透測試複雜許多，它不單要找出問題，還要同時找出硬體和軟體方面的問題。這個流程就與TARA結合得的非常緊密，通常是位於所謂「V模型」的右端。廠商必須通過徹底的檢驗來減少所有可能發生損害的情境，因為汽車一旦發生問題很可能會危及生命安全。

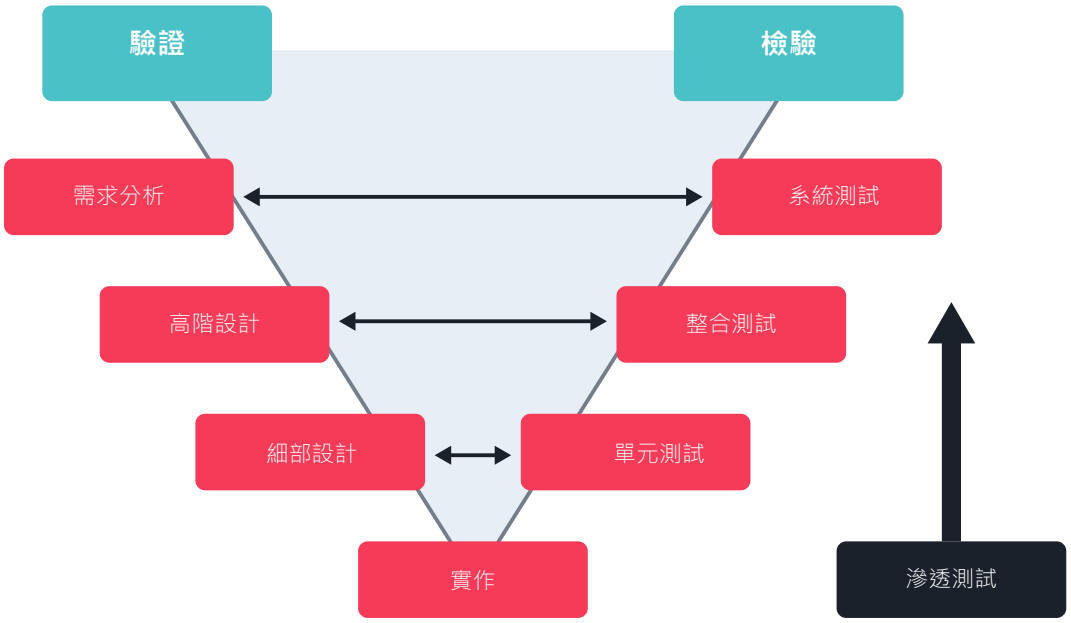

圖 10：汽車軟體開發的「V模型」。

風險管理

在汽車產業，風險管理是一個複雜的問題，涵蓋各種層面，包括：供應鏈、製造、法規、市場、金融、技術等等。其完整範圍遠比人們一開始想像的還大，汽車產業一般都投入了大量時間來發掘和評估風險，並且努力制定各種策略來加以防範，而過程當中也包含了持續的監控。所有的努力都只有一個目標，那就是在不斷演變的情勢當中確保長期的成就和安全。

安全是汽車產業至高無上的原則，傳統的車商通常更注重功能上的安全風險，而非網路資安風險。然而，隨著汽車逐漸朝軟體定義模型的方向演進，幾乎所有的功能都需要軟、硬體的配合，網路資安風險已成為一項最新的必要考量。對許多傳統汽車製造商來說，這是一個全新的領域，反映了不斷變化的情勢，讓汽車的功能和安全，與科技的整合越來越密不可分。適當的風險管理，甚至有助於TARA工作的推動，讓企業更容易達成法律的要求。

網路資安風險

所謂「網路資安風險」指的是系統因潛在的弱點或漏洞遭駭客攻擊而造成損害或遭到未經授權的存取。就汽車而言，這些漏洞並非只侷限於硬體，更涵蓋到軟體，漏洞可能出現在各種不同層次的汽車元件當中。例如，車內Wi-Fi連線管理員中的軟體漏洞，有可能變成駭客攻擊的入侵點。同樣地，一個看似簡單的漏洞，例如使用一個「軟體定義無線電」(SDR)裝置來記錄和回放無線射頻訊號，就可能讓駭客在不經過授權的情況下打開車門。這樣的風險彰顯出汽車產業網路資安複雜而多重面向的特性，廠商必須同時確保硬體與軟體的安全，才能有效保護系統，防範潛在威脅。

外部網路資安風險評估的關鍵挑戰就是將漏洞化為有價值的行動項目以防範風險，在汽車產業更是如此。近年來已經有人提出一些概念來解決這項問題，例如SBOM和HBOM。其中，SBOM的設計是要管理軟體供應鏈風險，而HBOM則是針對硬體供應鏈風險。當SBOM或HBOM當中所列的某個項目被發現漏洞時，企業就能迅速做出回應並有效加以防範。然而，這些流程的建置並非一件簡單的工作。雖然SBOM和HBOM的觀念理論上看似完美，但在真實世界裡，想要建立一套完整的SBOM或HBOM，卻是令人望之卻步的工作。其複雜性來自於今日汽車為數龐大的元件與相依性，以及同時追蹤所有軟、硬體潛在風險的困難度。

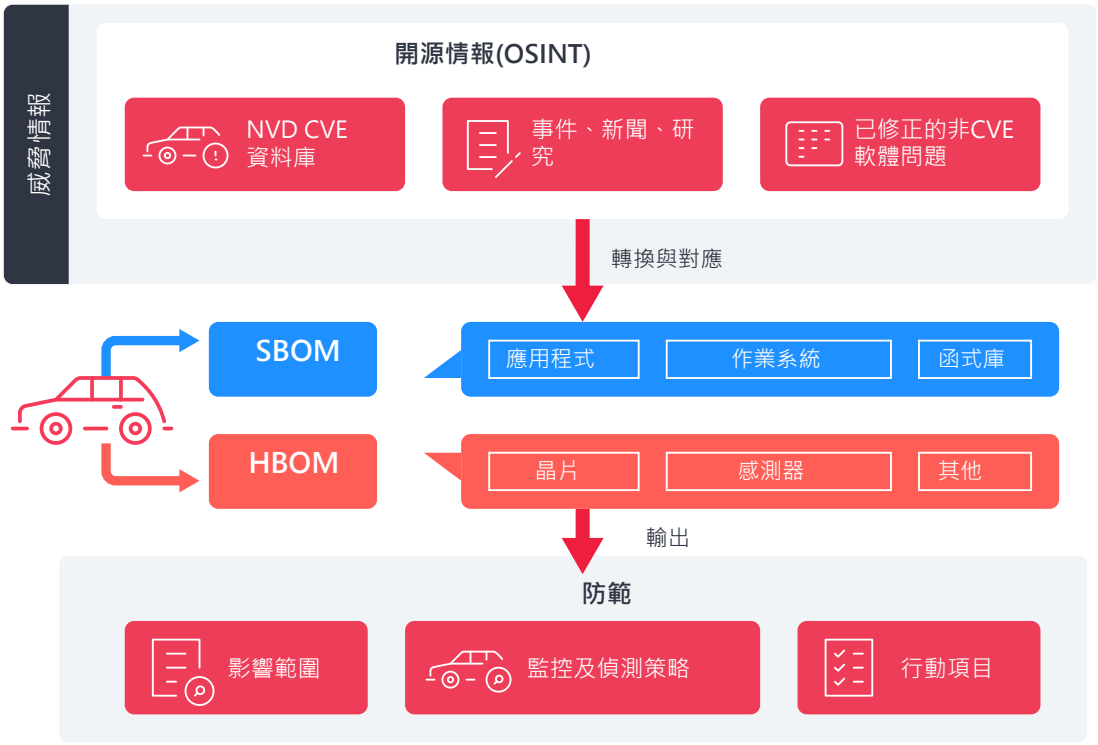

圖 11：外部網路資安風險的處理流程。

除了已知漏洞之外，通常還會有一些隱藏或較不明顯的漏洞會成為風險管理上的挑戰，尤其從廠商的角度來看。像這樣的例子包括：某篇研究論文提到的一個SSL函式庫的潛在漏洞，或使用工具來偽造「胎壓監測系統」(TPMS)的訊號。像這樣的隱藏風險，管理起來尤其困難，因為無法馬上就能偵測得到，或者加以掌握。廠商甚至根本不曉得這些漏洞存在，直到被駭客攻擊，或者有人做過詳細的研究為止。今日複雜的汽車技術，以及錯綜複雜的軟硬體互動，讓發掘與解決這些隱藏漏洞的工作變得更加複雜。

事件回應

所謂「事件回應」(IR)在IT產業通常指如何處理資安事件或網路攻擊所造成的效應，不過該詞在汽車領域的意義稍有不同，指的是如何同時因應外部的網路資安風險與內部的資安事件。比方說，當一家車廠在面對某個資安事件或網路攻擊時，它可能使用與IT領域相同的原則來降低衝擊。不論是發生在企業網路或公共雲端服務內部，作法是相同的。但是，如果問題牽涉到汽車，作法就必須有所不同。

在IT領域，一切都比較單純，當美國「網路資安與基礎設施安全局」(Cybersecurity and Infrastructure Security Agency，簡稱CISA)發出一項警告時，企業會對這項警告立即做出反應。即使該機構並未提供明確的行動方針，資安廠商也能迅速回應，因為IT產業有YARA、現成的教戰手則，以及MITRE框架這類工具可協助散播及尋找反制措施。

反觀汽車產業的情況就不同，如果某個廠牌的車被爆出一個漏洞，不論是因為發生事件或經由研究發現，其他車廠不會知道這項發現意味著什麼，也不知道這個漏洞是否會影響到他們的車款。沒有任何系統可以協助他們做適當的檢查，但他們卻可能想問以下幾個問題。

角色	問題	行動
產品安全事件回應團隊(PSIRT)	這個漏洞是否會影響我們的車款？	我們必須找出影響的範圍。
車輛安全營運中心(VSOC)	我們如何知道漏洞會不會發生？	監測是必要的，而且我們必須搞清楚如何加以偵測。

表 13：事件回應問題。

眼前汽車產業很難解決這兩個問題，因為沒有統一的標準。而且，各家車廠的情況也不盡相同，如果車廠確實掌握了自家車款的SBOM與HBOM，那事情就比較好辦，但並非所有車廠都是如此。毫無疑問地，汽車產業需要類似IT產業所用的技巧來快速面對並解決這些問題。

汽車數據生態系

除了法規遵循之外，汽車產業與汽車生態系也有一些領域突顯出法規本身也需要跟上產業的進步。一個明顯的例子就是汽車數據這個正在快速擴張、但卻被人忽略的領域。在趨勢科技前瞻威脅研究(FTR)團隊幫VicOne撰寫的一份報告「汽車數據：連網汽車領域的機會、變現盈利和網路安全威脅」(Automotive Data: Opportunities, Monetization, and Cybersecurity Threats in the Connected Vehicle Landscape)當中提到，這個生態系規模之龐大本身就是一個重大啟示[28]。

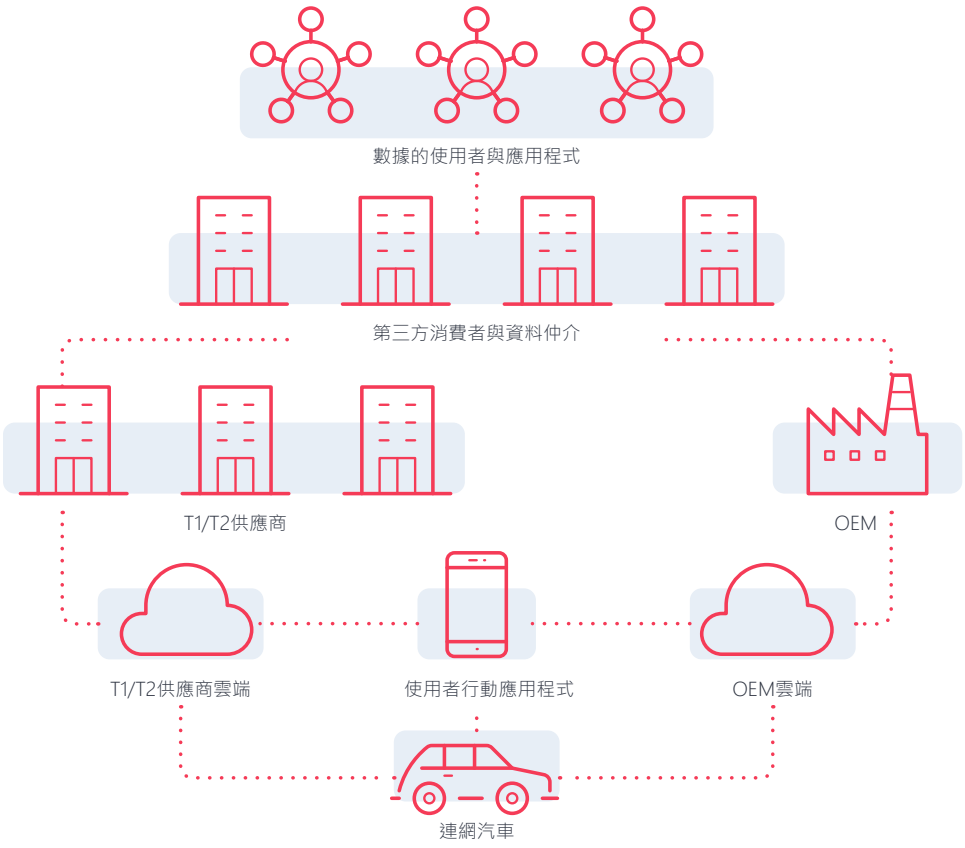

圖 12：汽車數據生態系。

雖然人們普遍理解今日的汽車會產生數據、也會使用數據，但對於當前汽車數據生態系真正的深度與複雜度卻大多缺乏認知。而這一點就反映在缺乏適當的法規標準可為該產業目前處理的大量數據提供明確指引。

數據營利方式在汽車產業的不斷進步，將帶來更強勁的營收成長，但也可能引來網路犯罪活動。如果這些數據被拿來營利的情況繼續成長下去，我們預料首波針對連網汽車的大規模攻擊將會衝著數據而來。我們不難預見這些數據一旦落入網路駭客手中將帶來什麼風險。雖然我們已經討論過汽車產業正如何學著應付網路資安法規的要求，汽車數據生態系象徵了該產業的進步如何突顯出當前法規的漏洞。汽車數據的蒐集與使用在立法上的漏洞必須獲得解決，汽車產業若要能明確妥善地處理這個日益成長的面向，就必須要有適當的立法。

汽車網路犯罪地下網路

觀察產業當前趨勢如何影響網路犯罪活動的另一種方法，就是到網路犯罪地下市場看看。為此，趨勢科技FTR團隊研究人員幫VicOne研究了地下市場當前及可預見未來可能出現的連網汽車網路犯罪形態[29]。

在這些論壇的討論中，最接近連網汽車網路攻擊的情況就是「改車」。改車通常是車迷在做的事，目的不外乎解鎖車子的某些功能或篡改里程數。他們會試圖開啟車子原本就內建的功能，例如開啟坐墊加熱功能(這功能對某些車廠來說屬於付費升級項目)，或者透過修改軟體來降低車子的里程數。雖然這類操作會影響OEM廠商的獲利，但並未真正攻擊到連網汽車的用戶，所以我們也有點質疑改車的行為是否該歸類為攻擊。

目前在地下論壇上廣泛討論的攻擊	未來在地下論壇上可能受到關注的攻擊
改車(自己動手修改車輛)，目的是： • 啟用一些付費功能，例如坐墊加熱功能。 • 篡改里程數。	當連網汽車使用者的帳號被賣給不肖集團後，歹徒會： • 利用網路釣魚、鍵盤側錄或其他惡意程式冒用使用者身分。 • 從遠端解鎖車門，或者啟動引擎或馬達。 • 打開車門將貴重物品洗劫一空。 • 將車開去從事一次性犯罪。 • 將車偷走拆解零件販賣。 • 跟蹤車子找到車主住址，進而知道車主是否在家。

表 14：目前我們在地下論壇上發現被廣泛討論的攻擊形態，以及未來在論壇上可能受到關注的攻擊形態。

另一個令汽車產業憂心的重大議題是針對OEM廠商的攻擊。我們已經發現一些駭客入侵廠商網路之後將虛擬私人網路(VPN)帳號賣到暗網上的例子。不過，將帳號賣到地下論壇只不過是駭客將IT資產轉變成獲利的一種典型方式，這顯示駭客集團尚未意識到連網汽車數據的價值，或者尚未看到這類市場需求。

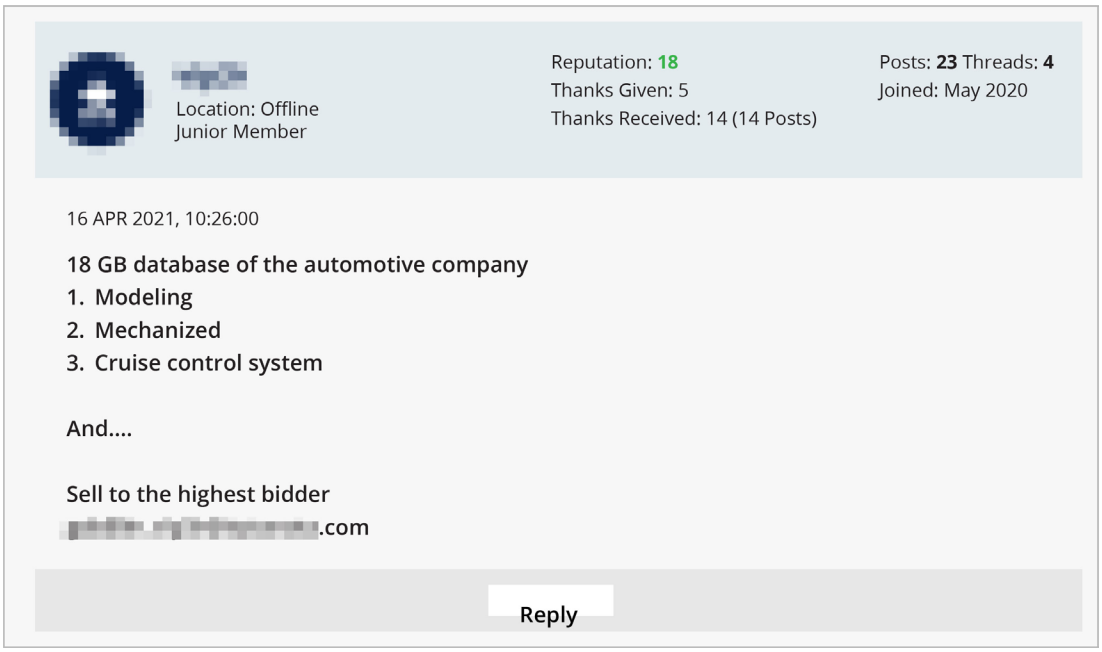

圖 13：網路犯罪地下論壇上某篇貼文在販賣從OEM廠商竊取到的數據(該貼文已被下架，此處為重製版本)。

從以上觀察可以看出，連網汽車數據在網路犯罪地下市場上的需求還在萌芽階段，不過我們預測這個階段不會持續太久。正如前面提到，我們預料當第三方機構開始廣泛運用汽車數據之後，連網汽車數據將變得非常值錢。網路犯罪集團很快就會意識到這點，而且不用多久就會開始冒出嘗試利用這些數據的犯罪。

SDV的未來前景：在創新與潛在疑慮之間取得平衡

SDV的出現，象徵汽車技術的重大進展，意味著汽車的能力、功能和整個駕駛體驗，更取決於軟體、而非硬體。儘管這項新興技術帶來了巨大的創新與客製化潛力，卻也帶來了諸多疑慮，尤其在安全、網路資安及資料隱私權方面。隨著汽車日益連網並仰賴軟體，它們也將更容易遭遇網路威脅與資料外洩事件，引來有關使用者敏感資料與汽車系統完整性的安全疑慮：

- 先進駕駛輔助系統(ADAS)：這類系統可透過自動煞車、車道維持輔助，以及主動式定速巡航控制(ACC)等等的功能來提升車輛安全。但這些功能得仰賴軟體和感測器來運作，使它們變成網路攻擊的目標，進而影響這些道路安全功能。

- 自動駕駛：自駕車擘劃了一個道路更安全、行車更有效率的未來。但自動駕駛系統的複雜性卻使得這類系統容易發生軟體問題以及駭客入侵的狀況，對乘客生命及資料安全造成風險。

- AI輔助智慧座艙：智慧座艙使用AI來提供個人化駕駛體驗，根據駕駛人的行為和偏好來調整設定。儘管這樣可以提升舒適度和便利性，但也引來有關個人資料蒐集和處理方式的疑慮，因此需要有嚴密的資料防護措施。

- 訂閱功能：汽車現在都提供了訂閱制的軟體功能，例如：更先進的導航與效能升級。這樣的商業模式要能運作，車輛必須與製造商持續交換資料，突顯出安全資料傳輸協定的必要，而資料的蒐集也必須更加透明。

- 依使用狀況計費的保險(UBI)：UBI會根據駕駛人的行為(透過車上的軟體隨時監控)來決定保險費率。這樣的作法需要蒐集詳細的駕駛資料，使得資料隱私權和安全又浮上了檯面，因為這些資料一旦遭到誤用或未經授權的存取，就可能嚴重影響個人隱私。

總結來說，雖然SDV創造了令人振奮的機會，但相關應用程式牽涉的人身安全、網路資安以及資料隱私權之間的複雜糾葛，需要一套全面而嚴密地監控方法來確保在符合安全和道德的方式下實現這些技術。

結論

在這份報告中，我們先檢視了法規的大環境，指出ISO/SAE 21434與UN R155至關重要。接著我們摘要說明了產業在法規遵循上所面臨的挑戰，這方面，OEM廠商或供應商可採用的作法視其當前的法規狀態與其對法規的經驗而定。不過，「設計上即具備安全」的核心指導原則應該貫穿整個製造流程。法規的目的是要確保每一個流程都符合安全，這樣才能在問題演變成災難之前預先加以處理。

在分析威脅情勢的過程中，我們注意到今年上半年網路攻擊所造成的損失金額已突破110億美元，相較於前兩年，可謂史無前例地暴增。仔細研究之後就會發現，這些網路攻擊絕大多數都是瞄準了汽車供應商，顯示此一趨勢正在崛起。令人憂心的是，這些攻擊有超過90%都並非瞄準OEM廠商本身，而是供應鏈上的其他單位。因為駭客普遍覺得資安嚴密的企業較不容易滲透，因此轉而瞄準警覺性較弱的企業。但OEM廠商同樣也會因為供應鏈中斷而受到影響，所以，防範網路攻擊的工作已經不再是保護好一家企業就行，而是要強化整體供應鏈。

此外，本文也透過案例研究來點出資安事件的本質，以及我們該如何透過技術與法規的手段來解決其根本問題。這些資安事件突顯了在每一個層次都執行檢驗的重要性，從個別元件到整合式系統。這證明了為何法規建議，尤其是ISO/SAE 21434與UN R155當中的TARA流程，對於尋找最佳工作流程來落實這項驗證流程非常關鍵。

隨著廠商開始跨入SDV領域，這項創新技術將使得汽車生態系發生革命性轉變，為汽車開拓更多元的使用方式。然而，這樣的發展也必然需要更好的資安措施來確保車輛的安全性。一個最明顯的例子就是汽車數據與持續擴張的汽車數據生態系，而這也點出了汽車產業的法規和規範在這方面的不足。新功能的推出經常會增加潛在的可攻擊面，汽車產業尤其是如此，所以任何的創新都應該要有強大的安全作為後盾。

參考資料

1. ISO. (2021). *ISO.* “ISO/SAE 21434:2021 Road vehicles Cybersecurity engineering.” Accessed on Nov. 17, 2023, at https://www.iso.org/standard/70918.html.
2. The MITRE Corporation. (April 25, 2009). *CWE.* “CWE-787: Out-of-bounds Write.” Accessed on Nov. 10, 2023, at https://cwe.mitre.org/data/definitions/787.html.
3. The MITRE Corporation. (July 19, 2006). *Common Weakness Enumeration.* “CWE-416: Use After Free.” Accessed on Nov. 10, 2023, at https://cwe.mitre.org/data/definitions/416.html.
4. The MITRE Corporation. (July 19, 2006). *Common Weakness Enumeration.* “CWE-125: Out-of-bounds Read.” Accessed on Nov. 10, 2023, at https://cwe.mitre.org/data/definitions/125.html.
5. The MITRE Corporation. (July 19, 2006). *Common Weakness Enumeration.* “CWE-120: Buffer Copy without Checking Size of Input (‘Classic Buffer Overflow’).” Accessed on Nov. 10, 2023, at https://cwe.mitre.org/data/definitions/120.html.
6. The MITRE Corporation. (July 19, 2006). *Common Weakness Enumeration.* “CWE-20: Improper Input Validation.” Accessed on Nov. 10, 2023, at https://cwe.mitre.org/data/definitions/20.html.
7. The MITRE Corporation. (July 19, 2006). *Common Weakness Enumeration.* “CWE-89: Improper Neutralization of Special Elements used in an SQL Command (‘SQL Injection’).” Accessed on Nov. 10, 2023, at https://cwe.mitre.org/data/definitions/89.html.
8. The MITRE Corporation. (July 19, 2006). *Common Weakness Enumeration.* “CWE-190: Integer Overflow or Wraparound.” Accessed on Nov. 10, 2023, at https://cwe.mitre.org/data/definitions/190.html.
9. Tavis Ormandy. (July 2023). *cmpxchg8b.* “Zenbleed.” Accessed on Nov. 10, 2023, at https://lock.cmpxchg8b.com/zenbleed.html.
10. Masaru Takada, Yuki Osada, and Masakatu Morii. (2019). *IEEE Xplore.* “Counter Attack Against the Bus-Off Attack on CAN.” Accessed on Nov. 10, 2023, at https://ieeexplore.ieee.org/document/8827010.
11. Matan Ziv. (June 2022). *Cymotive.* “CANCAN: Encapsulation of CAN-FD Messages for Circumvention of Security Measures.” Accessed on Nov. 10, 2023, at https://www.cymotive.com/wp-content/uploads/2022/06/CANCAN-Research-paper_-Matan-Ziv-Principal-Cybersecurity-Researcher-1.pdf.
12. Gedare Bloom. (Jan. 1, 2021). *NDSS.* “WeepingCAN: A Stealthy CAN Bus-off Attack.” Accessed on Nov. 10, 2023, at https://www.ndss-symposium.org/ndss-paper/auto-draft-102/.
13. Omar Yang. (May 5, 2023). *VicOne.* “How to Get Away With Car Theft: Unveiling the Dark Side of the CAN Bus.” Accessed on Nov. 10, 2023, at https://vicone.com/blog/how-to-get-away-with-car-theft-unveiling-the-dark-side-of-the-can-bus.
14. Ken Tindell. (April 3, 2023). *Canis Automotive Labs.* “CAN Injection: keyless car theft.” Accessed on Nov. 10, 2023, at https://kentindell.github.io/2023/04/03/can-injection/.
15. Ken Tindell. (April 3, 2023). *Canis Automotive Labs.* “CAN Injection: keyless car theft.” Accessed on Nov. 10, 2023, at https://kentindell.github.io/2023/04/03/can-injection/.
16. KeylessGoRepeater. (May 18, 2022). *WayBackMachine.* “Unlocker, opener for Toyota-Lexus 2017+.” Accessed on Nov. 10, 2023, at https://web.archive.org/web/20220518024120/https://keylessgorepeater.com/products/unlocker-opener-for-toyota-lexus-2017/.
17. KeylessGoRepeater. (May 18, 2022). *WayBackMachine.* “Unlocker, opener for Toyota-Lexus 2017+.” Accessed on Nov. 10, 2023, at https://web.archive.org/web/20220518024120/https://keylessgorepeater.com/products/unlocker-opener-for-toyota-lexus-2017/.
18. Shop-Auto-PODOLSK. (n.d.). *Shop-Auto-PODOLSK.* “AST PRO UNLOCKER for Toyota/Lexus (2017+).” Accessed on Nov. 10, 2023, at https://shop-auto-podolsk.com/ast-pro-unlocker-for-toyotalexus-2017/.
19. AutoDecoders. (n.d.). *AutoDecoders.* “AST PRO UNLOCKER for Toyota / Lexus 2017+.” Accessed on Nov. 10, 2023, at https://autodecoders.com/product/ast-pro-unlocker-for-toyota-lexus-2017/.
20. Agent Grabber. (n.d.). *Agent Grabber.* “Unlocker, opener for Toyota-Lexus 2015+.” Accessed on Nov. 10, 2023, at https://agentgrabber.com/en/product/unlocer-toyota-lexus-2020/.
21. Unlocks Cars Grabber. (n.d.). *Unlocks Cars Grabber.* “AST Unlock PRO: JBL Car Unlocking + Emergency Start for Toyota/Lexus.” Accessed on Nov. 10, 2023, at https://unlockcarsgrabber.com/product/ast-unlock-pro-jbl-car-unlocking-emergency-start-for-toyota-lexus/.
22. KodGrabber. (n.d.). *KodGrabber.* “(UST v1.0) Unlocker & Emergency start Toyota Lexus 2022.” Accessed on Nov. 10, 2023, at https://kodgrabber.club/keyprog/ust-v-10.
23. Numaan Huq, Craig Gibson, Vladimir Kropotov, and Rainer Vosseler. (Feb. 16, 2021). *Trend Micro.* “Cybersecurity for Connected Cars: Exploring Risks in 5G, Cloud, and Other Connected Technologies.” Accessed on Nov. 10, 2023, at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/in-transit-interconnected-at-risk-cybersecurity-risks-of-connected-cars.
24. Samwyco. (Jan. 3, 2023). *Sam Curry.* “Web Hackers vs. The Auto Industry: Critical Vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and More.” Accessed on Nov. 10, 2023, at https://samcurry.net/web-hackers-vs-the-auto-industry/.
25. Jaroslav Lobacevski. (March 21, 2022). *GitHub.* “Validate all the things: improve your security with input validation!” Accessed on Nov. 10, 2023, at https://github.blog/2022-03-21-validate-all-things-input-validation/.

26. United Nations. (June 24, 2020). *UNECE.* "WP.29 - Introduction." Accessed on Nov. 17, 2023, at https://unece.org/wp29-introduction.

27. Ben Ben-Aderet. (Feb. 17, 2023). *Forbes.* "The Five Important Moments In History That Shaped The Modern Cybersecurity Landscape." Accessed on Nov. 10, 2023, at https://www.forbes.com/sites/forbestechcouncil/2023/02/17/the-5-important-moments-in-history-that-shaped-the-modern-cybersecurity-landscape/.

28. Numaan Huq, Vladimir Kropotov, Philippe Lin, and Rainer Vosseler. (Nov. 15, 2023). *VicOne.* "Automotive Data: Opportunities, Monetization, and Cybersecurity Threats in the Connected Vehicle Landscape." Accessed on Nov. 15, 2023, at https://vicone.com/research/the-road-ahead-is-paved-with-risky-data.

29. Numaan Huq, Vladimir Kropotov, and David Sancho. (May 23, 2023). *VicOne.* "What Lies in Store for Connected Cars in the Cybercriminal Underground?" Accessed on Nov. 10, 2023, at https://vicone.com/blog/what-lies-in-store-for-connected-cars-in-the-cybercriminal-underground.

VicOne

Driving Automotive Cybersecurity Forward

VicOne致力保護未來車的安全，為汽車產業提供最新系列的車用資安軟體與服務。VicOne的解決方案專為滿足汽車製造商嚴格要求所設計，旨在保護並提供新型態汽車客製化的特殊需求。身為趨勢科技的子公司，VicOne憑藉著趨勢科技超過30多年在網路資安的堅固基礎，為客戶提供卓越的汽車防護與深度資安情報洞察，以協助建造安全又智慧的汽車。

更多關於VicOne訊息請參考：https://www.vicone.com/zh
或掃描以下 QR Code：