新通訊

Communication Components Magazine 元件雜誌

www.2cm.com.tw

掌握通訊產業脈動

特別企劃

疫情引爆企業專網商機 P. 7 9

5G助攻車聯網

NR-V2X帶動智慧交通革命 5G車聯網催生高度自駕

低延遲/高可靠/強資安防護 C-V2X滿足車規應用需求

總號第242期 NT$200

04/2021

ISSN 1608-747X

趨勢大追擊

打造全新LPWA生態圈

ZETA聯盟中/日二地異軍崛起

標準最前線

ISO/SAE 21434杜絕駭客威脅

汽車網路安全新標準底定

技術博學堂

行人預警/場域試運行雙管齊下

聯網自駕巴士安全上路就緒

提供STL實作內建自我測試

CPU力保汽車/工業功能性安全

MCU演算最佳化推進效率

雲端邊緣賦予電動車續航力

平穩切換內燃引擎/電動馬達

感測器解油電混合車難題

標準最前線

ISO/SAE 21434杜絕駭客威脅
汽車網路安全新標準底定

文 | Joseph Notaro

先進駕駛輔助系統(ADAS)有潛力使駕駛安全性遠高於當今。2015年，波士頓諮詢集團(Boston Consulting Group)估計，如果新車購買者投資當時可用且最常見的ADAS功能，則可以消除美國28%的車禍。隨著向自動駕駛汽車邁進技術的不斷改進，可預防的事故數量有望潛在拯救更多生命。

對於ADAS的發展至關重要的是，迅速改進的感測器技術。尤其是影像感測器，正在推動更高的ADAS效用。倒車攝影在停車時警告駕駛車後的障礙物。其他安裝在車身周圍的攝影機可為駕駛提供360度全方位視野，消除了在變換車道時導致事故的危險盲點。感測器技術越來越多地用於自動系統，以防止汽車陷入危險。先進特性如降低LED閃爍和高動態範圍等克服了不良照明條件引起的問題，否則這些問題會破壞ADAS演算法。

同時，汽車製造商正在利用感測器融合技術融合來自視覺影像、紅外線影像、雷達、光學雷達(LiDAR)和超音波影像的資料(圖1)。這樣，感測器可以補償會影響性能的情況，如在大霧、大雨中駕駛或當太陽接近地平線時。感測器網路結合先進的控制演算法，使不久的將來在高速公路上實現全自動駕駛的願景可行性提高。

汽車電控系統安全風險日增

電子感測和運算使用的增加帶來了風險。儘管融合可以處理啟用ADAS的車輛將面對的各種駕駛環境，但是如果它們處理的資料流程遭到破壞，則系統可能被迫產生異常的行為。感測器融合可以克服故障設備帶來的損壞，但更大的問題是故意篡改的問題，尤其是如果損壞是為了破解常規的糾錯常式而設計的。

駭客的攻擊已從理論轉變為真正的威脅，例如一些安全研究人員證明許多概念驗證性的駭客行為。迄今，概念驗證攻擊主要針對各個子系統，如控制引擎或試圖欺騙不同類型的感測器。還有日益嚴重的安全評估問題，是ADAS演算法日益複雜的性質，它正在轉向機器學習的形式。這樣一來，他們就容易遭受新形式的攻擊，如對抗性攻擊，在這種攻擊中，人們可能不會注意到的物理變化會完全改變汽車電子設備對情況的理解方式。

實際上，針對機器學習的對抗例子和類似攻擊構成的威脅有限，因為它們對鏡頭的遮鏡效果非常敏感，並且通常僅在特定距離才管用。感測器融合技術將在惡劣天氣條件下盡其所能提供一定程度的保護。但是，駭客可能會利用高度專注的技術作為更大策略的一部分：他們首先使用看似無關的攻擊來削弱整個系統的防禦能力，而針對機器學習系統的攻擊則是整個車輛無法以正確方式回應的弱點。

汽車中電子控制單元(ECU)和感測器模組的網路構成了完整的分散式電腦。對於攻擊者而言，如果不存在適當的防禦措施，那麼相互連結的模組會提供許多潛在的攻擊點。正如現已發現針對企業網路進行的駭客攻擊，可能涉及多種滲透方案，這些綜合起來會破壞系統的運行。

向駭客開放的攻擊類型可以有多種形式。基於篡改的攻擊可能涉及在車輛維護或閒入時插入的模組。損壞的模組用於透過車載網路發送感測器資料，進而誤導車輛做出不當決策。更改後的影像感測器模組可能會顯示亂序的幀或重播舊幀，進而使ADAS無法正確回應實際路況。

使用拒絕服務攻擊可更進一步進行物理攻擊：完全刪除對關鍵感測器的存取權限，或者使一個或多個模組生成大量垃圾，淹沒網路，進而使任何ECU都無法接收有效資料。或者，駭客可能會使用物理攻擊來削弱網路防禦，然後精由資訊娛樂子系統透過無線網路發起的遠端攻擊，來破壞透過安全開鍵網路發送的資料。

汽車OEM廠商面臨的問題是潛在攻擊的種類繁多，以及偵測每種攻擊的問題。篡改類型損壞的後續效應可能很難偵測到，因為它需要密切關注感測器模組之間的同步。如果發生拒絕服務攻擊，則車輛很可能必須停車才能進行任何類型的修復。

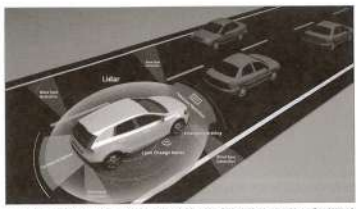

圖1 汽車製造商利用光學雷達偵測車輛周遭風險，再以感測器融合技術結合蒐集到的影像資料。

產業鏈共推標準
守護聯網車輛安全

為瞭解並解決與車輛網路安全相關的這些問題，ISO和汽車工程師協會(SAE)在2016年開始制定包括新的ISO/SAE 21434在內的許多標準。學術機構和其他機構與包括OEM、半導體公司、網路安全專家在內的82個參與者一起，於2020年初發布了第一份國際標準草案(DIS)，最終標準計畫於2020年底發布。

ISO/SAE 21434專注於影響安全性的汽車系統的網路安全層面。正在制定的標準遵循與ISO 26262類似的方法，該標準使用風險評估來辨識關鍵威脅並找到減輕威脅的方法，使用基於V形圖(V-diagram)的流程來管理其實施。它不強制要求產品或技術方案，但是與ISO 26262相同，它定義了從設計到退役，整個車輛生命週期必須遵循的流程。

由於現有標準並未充分涵蓋網路安全主題，因此ISO/SAE 21434將涵蓋車輛中的

隨著ADAS演算法漸趨複雜並導入機器學習，現今汽車電控系統的各子系統成為駭客鎖定的新目標。

所有電子系統、元件、感測器和軟體，並涵蓋整個供應鏈。為了符合新標準，汽車製造商和供應商必須能夠證明網路安全工程和網路安全管理已在整個設計中應用於相關供應鏈的所有元素。

V-diagram方法的使用為風險評估和緩解提供了分層解決方案，這將大幅有助於監視和抑制駭客攻擊。例如，安全協定很可能構成用於保護系統的底層技術的關鍵部分。在篡改和拒絕服務攻擊中，核心問題之一是被破壞的模組會影響系統運行，因為它們的輸出不受控制。網路上缺乏安全性還導致竊聽和重播攻擊，使用早前透過網路發送的資料。由於車載資料具有時效性，因此重複這些幀很容易破壞正確的運行。

為了防止對網路的攻擊並為車輛製造商提供遵循ISO/SAE 21434流程所需的支援，感測器和ECU製造商正著手整合安全協定，以使系統能夠檢查每個資料封包的資料完整性。業者如安森美半導體(ON Semiconductor)是已實施支援感測器元件中的資料加密、錯誤檢查和安全通訊的供應商之一。使用不可更改的時間戳記對資料封包進行加密和雜湊處理，可較容易拒絕重複的資料封包。不能正確回應加密挑戰的模組可以從網路中刪除，也可以將車輛置於自我保護(Limp-home)或固定模式，直到有問題的模組被刪除或替換為真實版本為止。

採取的其他方法包括支援特殊模式，如嵌入到矽片中的故障注入。這些為製造商和Tier-one整合商提供了測試程式和協定有效性的保證，以確保安全可靠的運行。

聯網安全標準法制化勢在必行

儘管新標準尚未被法律強制規定，但隨著新標準的發布，汽車製造商有望將其作為最佳實踐並向其供應商提出合規要求，這意謂著它將迅速成為未來聯網汽車的一部分。

儘管在標準最終定稿之前不能完全瞭解ISO/SAE 21434對個別產品的確切影響，但不可避免地會改變包括感測器在內的許多元件的軟體和硬體。這可能會導致新的符合ISO/SAE 21434的產品，或者是能夠聲稱符合該標準的現有產品的增強版本。安全設備和車輛的開發和測試方式肯定會發生變化。

至關重要的是，ADAS的安全益處不會因駭客問題的威脅而受到損害。有相關業者已在其整個產品開發過程中採用了多種標準，包括ISO/SAE 21434草案，以確保網路安全功能能夠應對使用感測器的系統可能遇到的威脅。如安森美半導體與業界合作，並幫助制定如ISO/SAE 21434等標準，助力實現安全性並兌現ADAS的承諾，為全自動駕駛汽車的未來鋪路。

(本文作者為安森美半導體全球汽車策略和業務拓展副總裁)